

DAVID Y. IGE  
GOVERNOR

JOSH GREEN  
LT. GOVERNOR

**STATE OF HAWAII  
OFFICE OF THE DIRECTOR  
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS**

335 MERCHANT STREET, ROOM 310

P.O. BOX 541

HONOLULU, HAWAII 96809

Phone Number: 586-2850

Fax Number: 586-2856

cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN  
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI  
DEPUTY DIRECTOR

**Testimony of the Department of Commerce and Consumer Affairs**

**Before the  
House Committee on Judiciary  
and  
House Committee on Consumer Protection and Commerce  
Tuesday, February 25, 2020  
3:00 p.m.  
State Capitol, Conference Room 329**

**On the following measure:  
H.B. 2572, H.D. 1, RELATING TO PRIVACY**

Chair Lee, Chair Takumi, and Members of the Committees:

My name is Stephen Levins, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department appreciates the intent of and offers comments on this bill.

The purposes of this bill are to: (1) redefine "personal information" for the purposes of security breach of personal information law; (2) establish new provisions on consumer rights to personal information and data brokers; (3) prohibit the sale of geolocation information and internet browser without consent; (4) amend provisions relating to electronic eavesdropping law; and (5) prohibit certain manipulated images of individuals.

The Department supports H.D. 1's expansion of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete. Businesses that collect or store data digitally have a responsibility

to protect information that is sensitive, confidential, or identifiable from access by hackers; these businesses also have a responsibility to prevent the data from being made available to criminals who engage in identity theft. As of 2018, all 50 states have data breach notification laws that prescribe when consumers must be notified when their “personal information” has been breached. Hawaii’s data breach notification laws were codified in 2006 as HRS chapter 487N, which, in pertinent part, defines “personal information” in relation to when a breach notification is required, and specifies the circumstances in which a business or government agency must notify a consumer that his or her personal information has been breached. Although Hawaii was one of the first states to enact this law, advancements in technology have made identity theft easier than it was 14 years ago. Businesses and government agencies now collect far more information, and bad actors exploit vulnerabilities in computer databases for nefarious purposes and with increased frequency.

H.D. 1 corrects existing statutory inadequacies by expanding the definition of “personal information” to include various personal identifiers and data elements, such as email addresses, health insurance policy numbers, security codes, and medical histories. This will enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including Vermont and California.

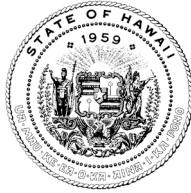
The Department also supports the consumer privacy protections in parts I and II of H.D. 1, as they require that consumers be afforded the right to provide their explicit consent before their identifying data may be used, shared, or sold. These safeguards are critically important in promoting consumer privacy.

Part III of H.D. 1 appears to model the regulation of data brokers in recently enacted legislation in Vermont and California. In addition to having a registration requirement, these laws provide consumers with the right to know what personal information is collected and sold about them, as well as the right to opt out of the sale of their personal information. While the underlying rationale for registering data brokers may be laudatory, the duties established in Part III -22 of the bill can be imposed without requiring registration. As such, the Department does not support Part III of H.D. 1 in its current form.

With respect to the other elements of H.D. 1, the Department believes that the bill's regulation of geolocation data as set forth in part IV will advance consumer privacy by prohibiting the sale of consumers' location data without their consent. Lastly, the Department takes no position regarding parts V and VI, since they primarily impact criminal enforcement.

Thank you for the opportunity to testify on this bill.

DAVID Y. IGE  
GOVERNOR



DOUGLAS MURDOCK  
CHIEF INFORMATION  
OFFICER

## OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119  
Ph: (808) 586-6000 | Fax: (808) 586-1922  
ETS.HAWAII.GOV

Testimony of  
DOUGLAS MURDOCK  
Chief Information Officer  
Enterprise Technology Services

Before the

HOUSE COMMITTEE ON JUDICIARY  
HOUSE COMMITTEE ON CONSUMER PROTECTION & COMMERCE  
TUESDAY, FEBRUARY 25, 2020

HOUSE BILL NO. 2572 HD1  
RELATING TO PRIVACY

Dear Chairs Lee and Takumi, Vice Chairs San Buenaventura and Ichiyama, and members of the committee:

The Office of Enterprise Technology Services (ETS) supports HB 2572 HD1, which redefines "personal information" for the purposes of security breach of personal information law, establishes new provisions on consumer rights to personal information and data brokers, prohibits the sale of geolocation information and internet browser information without consent, amends provisions relating to electronic eavesdropping law, prohibits certain manipulated images of individuals.

As chair of the Information Privacy and Security Committee created under HRS Section 487N, we support updating the definition of "personal information" to include expanded identifiers and data elements that are consistent with current and prevailing practices, as proposed in this bill.

Thank you for the opportunity to provide testimony on this measure.



February 25, 2020

Committee on Judiciary  
Rep. Lee, Chair  
Rep. San Buenaventura, Vice  
Chair

Committee on Consumer  
Protection and Commerce  
Rep. Takumi, Chair  
Rep. Ichiyama, Vice Chair

The House of Representatives  
The Thirtieth Legislature  
Regular Session of 2020

RE: HB 2572, HDI - RELATING TO PRIVACY  
DATE: Tuesday, February 25, 2020  
TIME: 3:00pm  
PLACE: Conference Room 329  
State Capitol 415 South Beretania Street, Honolulu HI

Aloha Chairs Lee and Takumi, Vice Chairs San Buenaventura and Ichiyama, and the Members of the Committees,

Thank you for the opportunity to testify in **support of part VI of HB2572 HD1** found on page 58 of the measure.

[SAG-AFTRA](#) represents over 1100 actors, recording artists, and media professionals in our state. We are the professional performers working in front of the camera and behind the microphone. We work in an industry that has seen tremendous advancement in the technology used to create and disseminate content. This evolution in content creation and distribution has not only led to an exponential growth in production and consumption of content, it has equalized the means of creation, broken down the barriers to entry and allowed for professional looking content created by almost anyone with determination and a smart phone.

However, there is a dark side to all this advancement. This dark side can be summed up by a new word that has entered our lexicon: Deepfakes. The same technology used to create younger versions of actors in movies, or insert actors who are no longer able to perform in movies due to death or unavailability, can now be used to create realistic non-consensual pornographic digital content. New technologies allow content creators to manipulate images to depict individuals as engaging in sexual activity or as performing in the nude without their consent or participation. Specifically, Internet users can use a publicly available artificial intelligence algorithm to transform still images of a person into live action performance by realistically inserting their face onto the body of a porn performer.

A recent Washington Post article, accessed [here](#), describes how “Fake-porn videos are being weaponized to harass and humiliate women: ‘Everybody is a potential target.’” Just as a smart phone has turned all of us into filmmakers with free and easily accessible distribution avenues (TikTok, Facebook, Instagram etc...), the same technology can be used to violate privacy, harass and abuse, turning unwilling people (mostly women) into porn stars.

Mericia Palma Elmore, Executive Director  
SAG-AFTRA Hawaii Local  
[mericia.palmaelmore@sagaftra.org](mailto:mericia.palmaelmore@sagaftra.org)  
Ph: 808-596-0388 • Fax: 808-593-2636  
201 Merchant St Suite 2301 Honolulu, HI 96813

SCREEN ACTORS GUILD - AMERICAN FEDERATION OF  
TELEVISION AND RADIO ARTISTS  
SAGAFTRA.org  
Associated Actors & Artistes of America / AFL-CIO

This proposed legislation amends HRS 711-1110.9 to include nonconsensual, digitally produced sexually explicit material, such as Deepfakes pornography, among the offences that constitute a violation of privacy in the first degree.

This amendment to HRS 711-1110.9 not only fits squarely within Hawaii's revenge porn laws, it also fulfills the constitutional mandate set forth in Section 6 of the Hawaii Constitution, requiring the legislature to take affirmative steps to implement rules that guarantee that the people's right to privacy be recognized and shall not be infringed.

We respectfully urge you to pass this section to protect not only our professional performers from exploitation, but to protect our daughters, sisters and mothers from this abusive violation privacy.

Thank you again for your continued support and please don't hesitate to contact the SAG-AFTRA Hawaii Local office for more information on this issue as it relates to professional performers.

Respectfully,

Mericia Palma Elmore  
Executive Director SAG-AFTRA Hawaii Local



February 24, 2020

The Honorable Chris Lee  
House Committee on Judiciary  
Hawaii State Capitol  
415 South Beretania St.  
Honolulu, HI 96813

**RE: HB 2572 - Relating to privacy**  
**OPPOSE**

Dear Chair Lee and Member of the Committee:

Internet Association wishes to respectfully express its opposition to HB 2572, which seeks to implement many of the diverse recommendations made by the 21st Century Privacy Law Taskforce from 2019. Due to the significant impact to the digital economy that these combined recommendations would have, and the fact that most of them have not yet been tested successfully in other jurisdiction, we request that you hold this bill in your committee.

Internet Association (IA) represents over 40 of the world's leading internet companies and advances public policy solutions that foster innovation, promote economic growth, and empower people through the free and open internet.

IA companies believe trust is fundamental to their relationship with consumers. Our member companies know that to be successful they must meet individuals' reasonable expectations with respect to how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and continually refining their consumer-facing policies so that they are clear, accurate, and easily understood by ordinary individuals. Additionally, our member companies have developed numerous tools and features to make it easy for individuals to manage the personal information they share, as well as their online experiences.

We urge you to hold HB 2572 in your committee. Several of the major provisions in this bill are taken from or inspired by California's recently enacted California Consumer Privacy Act of 2018 (CCPA). However, it does not make sense for Hawaii to mimic California's approach to privacy at this time given that the CCPA continues to be very much in flux. For example, CCPA's compliance requirements are currently being debated through the State's rulemaking process with the Attorney General, who has taken an expansive view and called for new obligations beyond those contemplated in the text of the law. Meanwhile, the original proponent of CCPA from 2018 is pushing yet another ballot measure in 2020 that would significantly change CCPA's provisions even further, creating more uncertainty for both businesses that must comply and for consumers who are supposed to benefit. This continuing uncertainty comes after businesses have invested millions of dollars and significant resources to meet



compliance deadlines and requirements in the current text of the statute. Given this turbulent situation with California's privacy law, it does not make sense for the State of Hawaii to rush and follow this approach.

Rather than a patchwork of state laws, internet companies support an economy-wide, federal privacy law that increases transparency and provides Americans meaningful control and the ability to access, correct, delete, and download data they provide to companies.

IA believes the time is right to modernize our federal rules and develop a national framework for consumer privacy. That framework should be consistent nationwide, proportional, flexible, and should encourage companies to act as good stewards of the personal information provided to them by individuals.

I appreciate your consideration and would welcome the opportunity to work with you, your colleagues and other stakeholders on crafting legislation which ensures data online privacy for all Hawaii residents and businesses. Please reach out to me if you have any questions. I can be reached at [rose@internetassociation.org](mailto:rose@internetassociation.org) or 206-326-0712.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rose Feliciano', followed by a long horizontal line.

Rose Feliciano  
Director, State Government Affairs Northwest Region



TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS  
IN OPPOSITION TO HB 2572, HB 1, RELATING TO PRIVACY

February 25, 2020

Honorable Representative Chris Lee, Chair  
Committee on Judiciary  
Honorable Roy M. Takumi, Chair  
Committee on Consumer Protection  
State House of Representatives  
Hawaii State Capitol, Room 329  
415 South Beretania Street  
Honolulu, Hawaii 96813

Chair Lee, Chair Takumi and members of the Committees:

Thank you for the opportunity to testify in opposition to HB 2572, HD 1, relating to Privacy.

Our firm represents the American Council of Life Insurers (“ACLI”). The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI’s member companies are dedicated to protecting consumers’ financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI’s 280 member companies represent 94 of the industry assets in the United States. ACLI members represent 95 percent of industry assets in the United States. Two hundred eighteen (218) ACLI member companies currently do business in the State of Hawaii; and they represent 95% of the life insurance premiums and 99% of the annuity considerations in this State.

The stated purpose of HB 2572 is to implement the recommendations of the Twenty-First Century Privacy Law Task Force set forth in its report which was submitted to the legislature on February 5, 2020.

The bill, among other matters, up-dates and expands what constitutes “personal information” for the purpose of Hawaii’s law governing the security breach of an individual’s personal information and establishes new provisions on consumer rights governing the use by businesses of her or his personal information, including its use and sale by data brokers.

The insurance industry is a consumer privacy leader in support of clear obligations in the appropriate collection, use and sharing of sensitive personal information. Given the sensitivity of the data that insurers collect from and about consumers insurers are subject to a prolific number of comprehensive federal and state privacy laws and regulations.

Consumers and companies need privacy requirements that are consistent and equivalent across state lines and provide equal protections to all consumers regardless of where they are located.

The financial services industry is uniquely and detrimentally affected by general privacy laws aimed at other industries as well as current privacy requirements. The complexities and expenses of implementing 50 differing state approaches to consumer privacy regulation is not, however, workable; and in some cases can include conflicting scopes, definitions, notice requirements and consumer rights.

Setting aside the difficulties we would face as an industry, differing approaches would be confusing and frustrating to consumers, with divergent rights to control their personal information based upon where they live or with whom they do business.

For the foregoing reasons ACLI believes that the only logical approach to the comprehensive regulation of the use of personal information – which applies equally and uniformly to all industries and provide rights and protections to all consumers over their personal information regardless of where they live – is the establishment of uniform preemptive national standards,

ACLI must, therefore, respectfully oppose HB 2572, HB 1, and urges your Committees to defer passage of this bill.

Again, thank you for the opportunity to testify in opposition to HB 2572, HD 1, relating to Privacy.

LAW OFFICES OF  
OREN T. CHIKAMOTO  
A Limited Liability Law Company

Oren T. Chikamoto  
1001 Bishop Street, Suite 1750  
Honolulu, Hawaii 96813  
Telephone: (808) 531-1500  
E mail: otc@chikamotolaw.com



February 24, 2020

Rep. Chris Lee  
Chair of the Committee on Judiciary  
Hawaii House of Representatives  
Hawaii State Capitol, Room 433  
415 South Beretania Street  
Honolulu, HI 96813

Rep. Roy M. Takumi  
Chair of the Committee on Consumer Protection & Commerce  
Hawaii House of Representatives  
Hawaii State Capitol, Room 320  
415 South Beretania Street  
Honolulu, HI 96813

**RE: Letter in Opposition to HI HB 2572**

Dear Chair Lee and Chair Takumi:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies in Hawaii and across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. We and the companies we represent strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies.

While we fully support the legislature's intent to provide Hawaiians with strong privacy protections, HB 2572 contains provisions that could harm consumers' ability to access products and services and exercise choice in the marketplace. The bill also contains particularly onerous terms surrounding digital data that could upend the Internet advertising ecosystem as we know it, disrupting consumers' online experience. Moreover, HB 2572 takes an approach that is highly inconsistent with other state privacy laws and privacy bills that are progressing through various state legislatures, while failing to develop a system that will work well for consumers or enhance a fair and competitive marketplace. In certain respects, the bill attempts to adopt definitions and structural elements of the California Consumer Privacy Act ("CCPA"). However, the CCPA is an incomplete statute, as the regulations implementing its terms have not yet been finalized. Furthermore, the CCPA contains various internal inconsistencies and ambiguities, and as such it should not be used as a basis for legislation in other states. For these reasons, we strongly oppose Hawaii's HB 2572.<sup>1</sup>

**I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth**

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect

---

<sup>1</sup> HB 2572, 30<sup>th</sup> Legislature, Reg. Sess. (Haw. 2020) (hereinafter "HB 2572").

and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.<sup>2</sup> Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.<sup>3</sup>

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.<sup>4</sup> It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design appropriate privacy safeguards—that we provide these comments.

## **II. The Bill's Definition of Personal Information for Breach Notification Purposes Extends Beyond Any State Law**

HB 2572 would greatly expand the definition of “personal information” subject to the state's data breach notification law by including identifiers in its scope.<sup>5</sup> Rendering such identifiers subject to the state's breach notification statute represents a massive expansion of breach notification requirements far beyond what any other state has done before. Even the CCPA does not include information used to identify individuals across technology platforms in its scope of information subject to the data breach enforcement provisions in the law.<sup>6</sup> Expanding Hawaii's definition of “personal information” for data breach notification in this way would make Hawaii be out of step with other states and cause a vastly increased number of notices sent to consumers, thereby unnecessarily raising consumer alarm without providing any additional privacy protections.

The definition of “personal information” for the purposes of Hawaii's breach notification statute should be comprised of data elements that could enable identity theft if misappropriated. Identifiers across technologies do not pose the same risks to consumers as other data elements that should rightly be

---

<sup>2</sup> John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017) <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

<sup>3</sup> *Id.*

<sup>4</sup> Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018) [https://www.ftc.gov/system/files/documents/advocacy\\_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400\\_ftc\\_comment\\_to\\_ntia\\_112018.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf).

<sup>5</sup> HB 2572, Part IV, § 4.

<sup>6</sup> Cal. Civ. Code § 1798.150(a)(1).

included in the scope of breach notification requirements. We therefore recommend that you not alter the definition of personal information for breach notification purposes.

### **III. The Bill Would Severely Impede Internet Commerce**

The bill would also require opt-in consent for any sale of geolocation information and “internet browser information,” defined as “information from a person’s use of the internet,” including web browsing history, application usage history, origin and destination IP addresses, device identifiers, and the content of communications comprising Internet activity.<sup>7</sup> This right to opt in to personal information sale is far different from other states’ approaches to personal information in the context of consumer privacy laws. If left uncorrected, HB 2752 would undermine the ad-supported Internet, crippling the online marketplace and resulting in a fractured experience for Hawaiian consumers.

Requiring opt-in consent for the sale of geolocation information and internet browser information would fundamentally change Hawaiians’ ability to access products and services they enjoy and expect through the Internet. Moreover, this approach is far out of step with other states’ consumer privacy proposals, such as the CCPA and others that impose an opt out regime to data sales rather than an opt in regime. HB 2572 defines “sale” broadly as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.”<sup>8</sup> As a result, any transfer of consumer data is likely a “sale” under the bill, which provides no customary exemptions for service providers or other entities that businesses rely on for various processing activities, and which a consumer would reasonably expect to receive personal information. Additionally, consumers would be inundated with requests for their consent to transfer internet browser information, thereby overwhelming them with a variety of notices and requests and causing significant consumer frustration.

Transfers of data over the Internet enable modern digital advertising, which subsidizes and supports the broader economy and helps to expose consumers to products, services, and offerings they want to receive. In a survey commissioned by the Digital Advertising Alliance, 90% of consumers stated that free content was important to the overall value of the Internet and 85% surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.<sup>9</sup> The survey also found that consumers value the ad-supported content and services at almost \$1,200 a year.<sup>10</sup> The opt-in requirements of HB 2572 could destroy this model, which consumers have expressed that they value and would not want to see replaced. We therefore respectfully ask you to remove the opt in consent requirements for “sales” of geolocation information and internet browser information.

### **IV. The Bill Could Cause Companies to Stop Offering Loyalty Programs in Hawaii**

The bill states that a business may charge a consumer a different price or rate or provide a different level or quality of goods or services if that difference is “reasonably related to the value provided to the business by the consumer’s personal information.”<sup>11</sup> The bill also states that a business may offer a different price, rate, level, or quality of goods or services to a consumer if the difference is

---

<sup>7</sup> HB 2572, Part IV, § 4.

<sup>8</sup> *Id.* at Part III, § -1.

<sup>9</sup> Zogby Analytics, Public Opinion Survey on Value of the Ad-Supported Internet (May 2016).

<sup>10</sup> Digital Advertising Alliance, Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid, PR Newswire (May 11, 2016).

<sup>11</sup> HB 2572, Part III, §§ -13(b), -26(b).

“directly related to the value provided to the business by the consumer’s personal information.”<sup>12</sup> These two requirements pose different standards, which will leave entities confused as to which one applies. Furthermore, these requirements are extremely ambiguous; business confusion regarding how to operationalize these requirements could cause many entities to forego offering loyalty programs in the state.

Hawaiians greatly benefit from loyalty and rewards programs and the price differences and discounts they receive for participating in those programs. The viability of loyalty programs is based on consumers’ participation in the aggregate. Consumer data powers loyalty programs and makes them worth it for the businesses that offer these programs. HB 2572’s terms limiting different price or service differences could impact businesses in their efforts to provide consumers with the loyalty and rewards programs they enjoy and expect. The bill does not provide any needed guidance regarding how a business may justify that a price or service difference is reasonably or directly related to the value of a consumer’s data. The bill also does not address how businesses may reasonably quantify nontangible value they receive from offering price or service differences through loyalty programs in terms of fostering consumer loyalty and goodwill. The lack of clarity on this issue could cause many businesses to decline to continue offering loyalty programs to Hawaiian residents.

For the foregoing reasons, we respectfully ask you to remove the unreasonable financial incentive requirements in the bill. In particular, we urge you to clarify or remove the provisions requiring businesses to ensure that financial incentives offered through loyalty programs are reasonably related or directly related to the value of the consumer’s data. These requirements are particularly unclear and therefore could be impossible to implement. Without additional clarity, HB 2572 could inhibit or drastically reduce the availability of loyalty programs offered in Hawaii.

## **V. The Bill’s Data Broker Requirements Are Broadly Applicable and Would Burden the State Government**

The bill proposes the creation of a data broker registry and provides consumers with rights to opt out from data brokers’ “sale” of personal information.<sup>13</sup> However, the term “data broker” is defined so broadly that it could encompass virtually any business that maintains data about Hawaiian consumers. “Data broker” under the bill means “a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the personal information of a consumer with whom the business does not have a direct relationship.” Combined with the definition of “sale,” a vast number of Hawaiian entities will be swept up in the scope of this definition and thus be subject to registration and other requirements. It was likely not the intent of the legislature to encompass virtually any entity doing business in Hawaii within the scope of the data broker requirements. We therefore encourage you to closely examine and limit the breadth of this definition.

Additionally, the data broker registration requirement provides little tangible protection for consumers. The disclosures required of data brokers pursuant to the bill are disclosures those data brokers already must make in privacy notices that are available to the general public. Obligating data brokers to provide a separate annual statement in regard to similar information could lead to confusing and outdated information in the market. Moreover, a data broker registry would create enormous new responsibilities for the Hawaiian government at a time when it is already considering taking on additional enforcement responsibilities in the context of passing omnibus privacy legislation. The data broker registration requirement in HB 2572 would add to these responsibilities by directing the office of consumer protection to create and manage a new registration system, complete with fee collection. This

---

<sup>12</sup> *Id.* at Part III, §§ -13(c), -26(c).

<sup>13</sup> *Id.* at Part III, §§ -21, -24.

would be a significant undertaking at a time when the government is considering broadly expanding its other responsibilities. We encourage you to carefully consider these impacts and update the bill so it does not contain a registration requirement.

\* \* \*

We and our members support Hawaii's commitment to provide consumers with enhanced privacy protections. However, we believe HB 2572 takes an approach that will severely harm the online economy without providing helpful privacy protections for consumers. We therefore respectfully ask you to reconsider the bill and update it to remove the terms we discussed in this letter so Hawaiians can continue to receive products, services, and offerings they value and expect over the Internet.

Thank you in advance for consideration of this letter.

Sincerely,

Dan Jaffe  
Group EVP, Government Relations  
Association of National Advertisers  
202-269-2359

Alison Pepper  
Senior Vice President  
American Association of Advertising Agencies, 4A's  
202-355-4564

Christopher Oswald  
SVP, Government Relations  
Association of National Advertisers  
202-269-2359

David Grimaldi  
Executive Vice President, Public Policy  
Interactive Advertising Bureau  
202-800-0771

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative  
703-220-5943

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation  
202-898-0089

# STATE PRIVACY AND SECURITY COALITION

---

February 25, 2020

Representative Chris Lee  
Chair, House Committee on Judiciary  
Hawaii State Capitol, Room 433  
Honolulu, HI 96813

Representative Roy Takumi  
Chair, House Committee on  
Consumer Protection and Commerce  
Hawaii State Capitol, Room 320  
Honolulu, HI 96813

**Re: HB 2572 (Oppose)**

The State Privacy & Security Coalition, a coalition of 30 leading telecommunications, technology, retail, payment card, online security, and automobile companies, as well as 8 trade associations, writes to strongly oppose HB 2572, a bill derived from the California Consumer Privacy Act (CCPA), and which also attempts to amend the state's data breach law, institute data broker reforms, regulate geolocation specifically, and regulate internet service providers. Moreover, HB 2572 contains outlier requirements that are overly prescriptive and do not reflect mainstream privacy and data security protocols.

As the state privacy landscape evolves, businesses of all sizes and consumers of varying levels of internet facility need understandable guidelines. A sixty-page piece of legislation that contains internal contradictions and will be literally impossible with which to comply will overwhelm both constituencies, costing businesses tens of millions of dollars in compliance costs, and confusing consumers.

## **I. CCPA Language**

### **CCPA is an Unfinished, Moving Target**

It does not make sense to introduce legislation in Hawaii that is based on unfinished and confusing legislation like the CCPA. Even as part of the law is now in effect, there are significant additional requirements that are still in doubt, both from 1) the interim Attorney General regulations (which have already changed twice and would add 25 pages of substantive new compliance obligations) and 2) the 2020 November Ballot Initiative, which aims to both correct errors and inconsistencies in the CCPA, and introduce additional requirements. If it passes in November, as expected, it will quickly make the existing CCPA obsolete.

Importantly, HB 2572 does not even reflect the amendments to CCPA that passed in October of 2019. These changed definitions, exempted employee information and added business-to-business regulations, and made an important change that allowed loyalty and discount programs to move forward.



## STATE PRIVACY AND SECURITY COALITION

In short, this unamended version of the CCPA, proposed by HB 2572, is so materially flawed that between last fall's amendments, as well as the AG's regulations, and the CCPA ballot initiative, this legislation will have been amended or changed eight times in the 26 months since its passage. Its ambiguities have led to the fact that since its passage in 2018, not a single state has enacted it. Neither Hawaii nor any other state should use it as a model.

Lastly, there currently three major pieces of federal privacy legislation being debated, and none of those three – proposed by Democratic and Republican members of a House Committee, a progressive Democratic Senator, and a conservative Republican Senator – use CCPA as a model or starting point, or incorporate any of its definitions.

### **CCPA Introduces Unintended, Negative Privacy Consequences**

The CCPA was passed with good intentions, but the lack of stakeholder input in the process created significant unintended consequences that incentivize anti-privacy behaviors in order to comply. HB 2572 would have the same effect.

First, HB 2572 strongly incentivizes the combination and storage of all personal information a company holds in one place to be able to comply with consumer rights requests, thereby also increasing vulnerability to hacking and fraud.

Second, because consumer data and consumer rights apply to a household as well as to an individual consumer, an abusive spouse can currently request all PI on his or her victim, and roommates can obtain financial account and social security number information about other roommates.

Third, the bill includes a fraud exemption only for the right to delete, thereby preventing a business which suspects the person submitting an access request is actually a fraudster from refusing the request. This is a data security threat and puts Hawaii consumers at serious risk of identity theft and other privacy harms.

### **CCPA Imposes Significant Compliance Costs on Business**

Not only does HB 2572 present anti-privacy consequences, it does so while imposing significant and unnecessary compliance costs on Hawaii businesses. In California, the State Department of Finance estimated that initial compliance costs for entities within the state would reach **\$55 billion**. This is not just limited to large businesses – the study estimated that approximately 75% of companies doing business in California would have to comply with the law. Businesses with 20 or fewer employees can expect to spend approximately \$50,000 to comply. For businesses with fewer than 50 employees, that number jumps to \$100,000.<sup>1</sup>

---

<sup>1</sup> [http://www.dof.ca.gov/Forecasting/Economics/Major\\_Regulations/Major\\_Regulations\\_Table/documents/CCPA\\_Regulations-SRIA-DOF.pdf](http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf)

# STATE PRIVACY AND SECURITY COALITION

## II. Data Broker Reforms

HB 2572 also proposes to institute data broker reforms. As we also point out below, it is not clear whether the CCPA language is intended to additionally apply to data brokers as well; given that the data broker law also contains consumer rights language, we assume that HB 2572 contemplates data brokers being regulated separately from any other business. However, that distinction is not made clear anywhere in the bill, and will be a compliance nightmare for businesses in the state that are not sure which regulatory scheme they will be required to abide by.

Moreover, the bill contains data security provisions that do not follow peer-reviewed and internationally accepted protocols, such as the National Institute for Standards and Technology Cybersecurity Framework, or the International Organization for Standardization (ISO) certifications. These frameworks encourage entities to evaluate their own organizations with regard to any number of cybersecurity risks, and to prioritize and tailor their solutions to the highest-level risks for their customers and employees.

Instead, HB 2572 sets forth draconian requirements that, while they may be implemented already by large entities, would be crippling to implement for small businesses (for instance, anti-fraud vendors who track suspected fraudsters and provide information to their customers). The types of data security controls that a given organization should use, and the circumstances for which they should use them, are best left to the types of international standards bodies mentioned above.

## III. Geolocation Information & Internet Browser Information

The bill also attempts to specifically legislate both geolocation information and ISP privacy. As we reference above, it is incredibly confusing to propose comprehensive legislation for all types of personal information in one way – via the CCPA language – and then segregate two particular types of data in an entirely different section of the bill.

### a. Geolocation Data

Section 4 is broad and ambiguous in a way that is likely to have unintended consequences. The Federal Trade Commission's (FTC) 2012 privacy framework notes that precise geolocation is sensitive information for which an entity should receive consent before using, and we do not oppose such a requirement. However, any bill attempting to regulate this should be carefully considered. For instance, there is no fraud exemption here, so that fraudsters could refuse to be tracked and avoid triggering red flags in systems that use location as an element that subjects suspicious transactions to closer inspection and identify patterns that help to prevent future unlawful activities.

Similarly, there is no exception for emergency services, or any health-related activities where a person is disabled and cannot provide consent, and where an entity's transfer of information to another entity (a "sale" under this bill) would mean the literal difference between life and death.

## STATE PRIVACY AND SECURITY COALITION

These problems will likely ensue due to the use of the CCPA definition of “sale” – a definition which is at the heart of most of CCPA’s unintended consequences. Using this definition in this context will almost surely cause similar unintended consequences. For example, if a consumer requests a transaction that involves the disclosure of location information from a business to its service provider, must the consumer provide express consent to do so? What if the consumer requests such a transaction but does not provide the consent necessary to complete the transaction?

HB 2572 is also broad enough to include every photograph or video that is captured by a phone and transferred by a photo application to a cloud storage company. It could also include any information that contains a consumer’s zip code, which would provide some broad sense of a consumer’s location; or information that contains a customer’s purchase history but does not include geolocation information. These types of unintended consequence should be avoided.

Of course, Hawaii is a unique and treasured tourist destination. The Hawaii Tourism Authority estimated that in 2017, 9.3 million tourists visited. If every tourist took even 5 photos, that would be 46.5 million photos generated. Subjecting each one of these to enforcement as a result of, for example, a consumer transferring a photograph from a consumer’s email account to his or her social media account is likely not what the legislature intends to regulate, but applying the CCPA’s definition of “sale,” that is exactly what would occur.

### **b. Internet Browser Information**

The latter part of section 4 departs from the FTC’s Privacy Framework, because browsing history is not considered sensitive information, and because different segments of such information are frequently transferred to keep the provision of services free, as well as to detect suspicious and fraudulent activity that harms individuals conducting legitimate online activity.

This provision also creates inconsistencies with the CCPA definition of “personal information” earlier in the bill, which explicitly includes internet browsing activity and internet protocol addresses. Of course, the CCPA does not require opt-in consent to collect or use these types of information, meaning that a business is permitted to transfer this information to another entity under one provision of HB 2572, but prohibited from doing so without consent under a different provision of the same bill.

Similar to the problems created by using the CCPA definition of “sale” with geolocation information, using the definition of “sale” here fails to recognize the modern online ecosystem. The bill would impose unreasonable and unwarranted obligations before an internet service provider or any other entity could perform functions that are likely well within the consumer’s expectations.

If consumers do not opt in to uses of data that permit companies to develop new products and services, or to certain sharing of cybersecurity threat information, both businesses and consumers will suffer. Similarly, much of the free news and content that is available online is supported by

## STATE PRIVACY AND SECURITY COALITION

advertising, which takes place through the exchange of pseudonymous identifiers. This presents little risk to individuals, who may already opt out of the use of their data for most advertising purposes.<sup>2</sup> Requiring consumers to opt in to these low-risk uses of information that characterize the flow of online services is likely to impact these free services that consumers have come to enjoy.

In conclusion, HB 2572 is a sprawling piece of legislation that will be nearly impossible to comply with and impossible for both businesses and consumers to understand. We would be willing to work with your committees on a better alternative that achieves the same comprehensive goals but is much simpler and provides more meaningful consumer benefits.

Respectfully submitted,



Andrew Kingman  
General Counsel  
State Privacy and Security Coalition

---

<sup>2</sup> See, e.g., Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 40-44 (2012); CAN-SPAM CITE; Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at: <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; Network Advertising Initiative Code of Conduct (2018), available at: [http://www.networkadvertising.org/sites/default/files/nai\\_code2018.pdf](http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf).



Feb. 25, 2020

Reps. Chris Lee and Roy Takumi  
House Judiciary and Consumer Protection Committees  
Honolulu, HI 96813

Re: House Bill 2572, HD1

Chairmen Lee and Takumi and Committee Members:

The Hawaii Professional Chapter of the Society of Professional Journalists appreciates the opportunity to comment on this bill.

We fear that Part III of the measure could affect a reporter's job of collecting information because persons could claim the reporter was harassing them by just contacting them. The provision prohibits anyone from obtaining personal information for the purpose of stalking or harassment but does not define harassment.

We ask that you incorporate a reference to the criminal definition of harassment by stalking ("without legitimate purpose") in §711-1106.5

Thank you for your time and attention,

Stirling Morita  
President, Hawaii Professional Chapter of the Society of Professional Journalists

February 24, 2020

Representative Chris Lee  
Chair, House Committee on Judiciary  
415 S Beretania Street  
Room 433  
Honolulu, HI 96813

**RE: H.B. 2572 Relating to Privacy – ETA Comments – Privacy and Fighting Fraud**

Dear Representative Lee:

On behalf of the Electronic Transactions Association (“ETA”), we appreciate the opportunity to provide comments on the use of data to fight fraud. The payments industry makes dedicated efforts to use innovation to fight fraud and ensure that consumers have access to safe, convenient, and affordable payment services. ETA and its members strongly support a privacy framework that allows companies to implement innovative tools to protect consumer privacy and data while fighting fraud. While ETA prefers a uniform national approach to privacy rather than a patchwork of disparate state requirements, if policymakers would like to institute a state law in Hawaii, ETA requests that any law allow for an explicit exemption for permissible use of data for purposes of detecting and protecting against fraud and for entities that are subject to the federal Gramm-Leach-Bliley Act and implementing regulations.

ETA is the leading trade association for the payments industry, representing over 500 payments and financial technology (“FinTech”) companies that offer electronic transaction processing products and services and commercial loans, primarily to small businesses. During 2018 in North America alone, ETA members processed over \$7 trillion in consumer purchases. ETA members include financial institutions, payment processors, FinTech companies, and all other parts of the payments ecosystem.

**Executive Summary**

ETA and its members support U.S. and international efforts to strengthen privacy laws to not only help industry combat fraud but also disclose to consumers how their data is being used. As lawmakers and regulators explore additional ways to protect consumers, it is critical that government coordinate with the payments industry so that companies can continue to combat fraud and cybercrime and ensure consumers have access to safe, convenient, and affordable payment options and other financial services.

There are numerous existing consumer protection laws in the U.S. and around the globe that address data security and privacy, and which align with the payments industry’s fraud fighting efforts. In the U.S., for example, financial information data is governed by federal laws, including the Gramm-Leach-Bliley Act and the related Federal Trade Commission’s Safeguards Rule and the Consumer Financial Protection Bureau’s Privacy Rule, as well as robust self-regulatory programs like the Payment Card Industry Data Security Standard, which sets forth requirements

designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. All of these laws and self-regulatory efforts recognize the critical role played by industry in combatting fraud, and they include provisions that allow for the targeted use and sharing of information by financial institutions and payments companies to protect consumers and to prevent fraud from occurring in the first instance.

Moving forward, ETA encourages policymakers to consider ways that law enforcement and industry stakeholders can continue to work together to develop new ways to combat rapidly evolving and increasingly sophisticated fraud and cybercrime. Working together, lawmakers, regulators, and the payments industry have kept the rate of fraud on payment systems at remarkably low levels. By continuing to collaborate, government and industry can provide consumers with access to safe and reliable payment services. As different states and the federal government consider this important issue, it is important for policymakers to work together across state-lines to provide a consistent privacy framework without creating a patchwork of conflicting regulations.

### **The Role of the Payments Industry in Fighting Fraud**

The payments industry is committed to providing consumers and merchants with a safe, reliable, and modern payments system. Indeed, consumers continue to choose electronic payments over cash and checks because of the protections afforded by electronic payments. These protections include, for example, zero liability for fraudulent charges, making electronic payments the safest and most reliable way to pay.

When it comes to credit cards, for example, a consumer can submit a chargeback request to his or her card issuing bank disputing a particular transaction. This process protects consumers and ensures that the financial institution bears ultimate responsibility for fraudulent transactions, demonstrating the industry's strong interest in making sure fraudulent actors do not gain access to payment systems.

In addition, the payments industry has a long history of fighting fraud through robust underwriting and monitoring policies and procedures, and the use of advanced authentication technologies. With the benefit of decades of expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems, monitor the use of those systems, and terminate access for network participants that engage in fraud. Working with its members and industry and government stakeholders, ETA has published various guidelines that provide underwriting and diligence best practices for merchant and risk underwriting, including the "Guidelines on Merchant and ISO Underwriting and Risk Monitoring" and "Payment Facilitator Guidelines," which provide information on anti-fraud tools, security, and related issues. When it comes to card data protection, the payments industry took the lead in developing the Payment Card Industry Data Security Standard ("PCI-DSS") to ensure the safety of cardholder data. The PCI-DSS sets forth requirements designed to ensure companies that process, store, or transmit credit card information maintain a secure environment for such data. In addition, the PCI-DSS establishes a framework for implementation of those data security standards, such as assessment and scanning qualifications for covered entities, self-assessment questionnaires, training and education, and product certification programs.



ETA members are constantly developing and deploying new technology and tools to detect, deter, and eliminate fraud. Just a few examples of these efforts include the following:

- **Data Encryption.** The payments industry has introduced point-to-point encryption (P2PE) and the tokenization of data to minimize or eliminate the exposure of unencrypted data in connection with a purchase.
- **Improved Authentication.** The use of new authentication methods to verify and authenticate transactions helps minimize potentially fraudulent transactions.
- **Fraud Scoring / Suspicious Activity Monitoring.** The payments industry continues to refine tools for monitoring and analyzing payment data for suspicious activity. With improvements in machine learning and artificial intelligence, the payments industry gains additional tools for identifying suspicious patterns in transaction data.
- **Chip Cards and EMV.** The payments industry has worked to replace magnetic stripes for credit and debit cards with a computer chip card, also called EMV. Chip cards make our payments system stronger by protecting against theft, counterfeit cards, and unauthorized use of cards in stores.

These are just some of the tools that the payments industry has developed in recent years to fight fraud, protect consumers, and ensure the integrity of the payments ecosystem. These efforts have been remarkably successful in reducing fraud while ensuring that consumers have access to fast, reliable, and safe payment options. Policymakers should consider that fraud prevention is not done through a static approach, but a dynamic and responsive approach that requires a regulatory framework that allows companies to respond to new threats in new ways.

### **ETA Supports a Uniform Regulatory Framework that Recognizes the Efforts of Industry to Fight Fraud and Protect Privacy**

ETA and its members support U.S and international regulatory efforts that encourage and respect industry efforts to combat fraud and disclose to consumers how their personal information is being used. Working together, lawmakers, regulators, and the payments industry have had remarkable success in protecting consumers and providing them with access to safe and convenient payment systems. This is achievable because the existing legal framework for protecting consumer privacy recognizes the important role of industry efforts in preventing and fighting fraud.

In the U.S., for example, laws have been passed to protect health information (HIPAA) and financial information (Gramm-Leach-Bliley Act and Fair Credit Reporting Act), and marketing activities are regulated through federal and state competition laws, as well as industry and activity specific laws, such as the Telephone Consumer Protection Act, Telemarketing Sales Rule, and CAN-SPAM regulations. These laws recognize the important role that industry plays in combatting fraud and provide provisions that allow for the targeted use and sharing of data to protect consumers and to prevent actual or potential fraud from occurring in the first instance.



## Consumer Protection Laws and Provisions Related to Industry Fighting Fraud

**Gramm Leach Bliley Act ("GLBA"):** The GLBA requires financial institutions to explain their information-sharing practices to customers and safeguard sensitive data. The GLBA has an exception to its information-sharing restrictions for information disclosed to "protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability."<sup>1</sup>

**Bank Secrecy Act ("BSA"):** The BSA establishes various requirements for covered financial institutions to assist the government in identifying and combatting money laundering and terrorist financing. The BSA includes numerous provisions governing the sharing of information between covered financial institutions and law enforcement, as well as sharing of information between financial institutions in order to identify and report activities that may involve terrorist activity or money laundering.

**Health Insurance Portability and Accountability Act of 1996 ("HIPAA"):** This law provides data privacy and security provisions for safeguarding medical information. Under the HIPAA Privacy Rule, a covered entity can disclose protected health information to detect fraud, abuse, or compliance violations.

**Federal Trade Commission ("FTC") Act:** Section 5 of the FTC Act prohibits unfair or deceptive business acts or practices, including those relating to privacy and data security. The FTC has recognized the need for industry to share information in order to fight fraud. In a 2012 privacy report, the FTC identified "fraud prevention" as a category "of data practices that companies can engage in without offering consumer choice" because they are "sufficiently accepted or necessary for public policy reasons."<sup>2</sup>

**The Fair Credit Reporting Act ("FCRA"):** The FCRA establishes a framework for the use and sharing of consumer reports and requires covered entities to develop and implement an identity theft prevention program. While not an explicit exemption, it has traditionally been understood that consumer information disclosed for the purposes of fraud prevention is not "consumer report information" subject to the restrictions of the FCRA.<sup>3</sup>

**Telephone Consumer Protection Act ("TCPA"):** The TCPA was designed to safeguard consumer privacy by regulating telemarketing using voice calls, text messaging, and faxes. In 2015, the Federal Communications Commission exempted from the TCPA calls from financial institutions intended to prevent fraudulent transactions, identity theft, or data breaches.<sup>4</sup>

<sup>1</sup> 12 C.F.R. § 1016.15(a).

<sup>2</sup> FTC, Protecting Consumer Privacy in an Era of Rapid Change, available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> at 36 (2012); see also id. at 39 (reaffirming this preliminary conclusion following review of public comments).

<sup>3</sup> This view was supported by the court's decision in *Kidd v. Thomson Reuters Corp.*, 299 F. Supp. 3d 400 (S.D.N.Y. 2017), which concluded that Thomson Reuters was not a "consumer reporting agency" by virtue of a service that disclosed information to customers for fraud prevention purposes.

<sup>4</sup> See *In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.* <https://www.fcc.gov/document/tcpa-omnibus-declaratory-ruling-and-order>, CG Docket No. 02-278, July 10, 2015 at ¶ 129.

Likewise, the legal frameworks in Europe and Canada respect the need for industry to share personal information in order to protect consumers from fraud. In Europe, the General Data Protection Regulation (GDPR) recognizes the important role that industry plays in fighting fraud and expressly permits (a) “processing of personal data strictly necessary for the purposes of preventing fraud,”<sup>5</sup> and (b) decision-making based on profiling that is used for fraud monitoring and prevention consistent with law. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) allows for the sharing of personal information without consent if it is “made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud. . . .”<sup>6</sup>

As lawmakers and regulators continue to explore new ways to protect consumers, ETA and its members encourage them to collaborate with industry to ensure that new laws and regulations are appropriately tailored to address specific needs – this ensures a balance between protecting consumers and allowing industry room to innovate and develop new and beneficial security practices and fraud detection and mitigation tools.

### Conclusion

The payments industry never rests. We work tirelessly to fight fraud and protect consumers, including by developing new tools and solutions to prevent, identify and fight fraud by analyzing data. Privacy laws should recognize these goals and the important role the payments industry plays in combatting fraud. By working together, lawmakers, regulators, and industry can protect consumers while providing them with access to the safest and most convenient payments system in the world.

Thank you for the opportunity to participate in the discussion on this important issue. If you have any additional questions, you can contact me or ETA Senior Vice President, Scott Talbott at [stalbott@electran.org](mailto:stalbott@electran.org).

Sincerely,

Tom Bloodworth  
State Government Affairs  
Electronic Transactions Association  
[TBloodworth@electran.org](mailto:TBloodworth@electran.org)  
(731) 414-3415

---

<sup>5</sup> European Union, GDPR, Recital 47.

<sup>6</sup> PIPEDA, Available at <https://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/118084/sc-2000-c-5.html>.



**SanHi**

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: February 24, 2020

TO: Representative Chris Lee  
Chair, Committee on Judiciary

Representative Roy Takumi  
Chair, Committee on Consumer Protection & Commerce  
*Submitted Via Capitol Website*

FROM: Rick Tsujimura

RE: **H.B. 2572, H.D. 1 - Relating to Privacy**  
**Hearing Date: Tuesday, February 25, 2020 at 3 p.m.**  
**Conference Room: 329**

---

Dear Chair Lee, Chair Takumi and Members of the Committee on Judiciary and the Committee on Consumer Protection and Commerce:

I am Rick Tsujimura, representing State Farm Mutual Automobile Insurance Company (State Farm). State Farm offers these comments about [H.B. 2572, HD1 Relating to Privacy](#).

State Farm understands and shares the Legislature's concern for protecting the privacy of information that consumers give to businesses to allow the businesses to provide the products and services that consumers desire. There are numerous Federal and State laws that provide such protections. With that in mind, below are some specific comments and suggested amendments:

1. P. 5, // 19-20, defining a social security as a "specified data element." A normal practice to mask a social security number is to truncate it to include only the last four digits. State Farm recommends striking the following: "~~either in its entirety or the last four or more digits~~".
2. P. 6, / 3: as written, it is unclear how "individual" is being used as a modifier. It could be rewritten to read: "An **individual's** individual taxpayer identification number".
3. P. 7, // 5-19: encryption is a recognized method of protecting personal information, and this was included in existing 487N-1. State Farm recommends including it by amending / 16 as follows: "elements **when either the identifier or the data elements are not encrypted**".

4. P. 12, /, 1: the definition of “consumer” is over-inclusive by including individuals in their capacity as “employees.” State Farm recommends adding the following after “State” and before the “.”: **“but not in the individual’s capacity as an employee”**.
5. P. 12, //, 5-17: the definition of “data broker” seems overly broad—it is not limited strictly to the sale of information and the definition of licensing information is broad enough that it could be construed to loop in businesses that wouldn’t typically be data brokers.
6. P. 15, /, 1-P. 16, /, 21: the definition of “personal information” “Consumer Privacy” Act. Although the “publicly available” is defined (p. 16, //, 18-21), the definition does not exclude that information from “personal information,” as does the definition on page 7 of the bill. State Farm recommends adding the following to P. 15, /, 1 after “that”: **“is not publicly available and that”**.
7. P. 29, /, 19-P. 30, /, 2: This is the Gramm-Leitch-Bliley Federal pre-emption provision. The last clause after “regulations,” /, 1, page 30, creates ambiguity, and for this reason it was left out of the versions of this legislation that other states have adopted (see, e.g., the California version codified at Cal.Civ.Code §1798.145(e)). State Farm recommends deleting the following: **“, to the extent this part is in conflict with that law”**.

Thank you for considering these comments and suggestions.

## **TESTIMONY OF MICHAEL TANOUE**

---

### **COMMITTEE ON JUDICIARY**

Representative Chris Lee, Chair

Representative Joy A. San Buenaventura, Vice Chair

### **COMMITTEE ON CONSUMER PROTECTION & COMMERCE**

Representative Roy M. Takumi, Chair

Representative Linda Ichiyama, Vice Chair

Tuesday, February 25, 2020

3:00 p.m.

### **HB 2572, HD1**

Chair Lee, Vice Chair San Buenaventura, and members of the Committee on Judiciary, and Chair Takumi, Vice Chair Ichiyama, and members of the Committee on Consumer Protection & Commerce, my name is Michael Tanoue, counsel for the Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit association of property and casualty insurance companies licensed to do business in Hawaii. Members companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

The Hawaii Insurers Council offers comments regarding, and requests one amendment to, the bill.

The Hawaii Insurers Council commends your Committees' effort to protect the personal information of consumers in Hawaii. However, Sections 2, 3 and 4 of the bill unreasonably impair the ability of insurance licensees to conduct their business of providing insurance products and services to Hawaii consumers, and these sections unnecessarily regulate insurance licensees in a field already adequately regulated by the Insurance Code (Chapter 431 of the Hawaii Revised Statutes) and ably overseen by the Insurance Division. For example and more specifically, the insurance industry in Hawaii is already subject to strict statutes requiring insurance licensees to inform consumers of their privacy rights and to safeguard consumers' nonpublic personal information, as well as Hawaii

Supreme Court decisions protecting consumers' state constitutional right of privacy in their health information.

In addition, in the Hawaii Insurers Council's view, an exception for "publicly available" information should be more clearly set forth in the definition of "personal information."

Accordingly, the Hawaii Insurers Council first requests that insurance licensees (including property and casualty insurers) be exempt from Section 3, Part II of the bill (starting on page 18, line 6, through page 30, line 9). Specifically, the Hawaii Insurers Council requests that the following provision, exempting insurance licensees from Part II of the bill, be inserted:

§ -17 Part not applicable to insurance licensees. This part shall not apply to any insurance licensee as defined in section 431:3A-102.

Section 431:3A-102 defines the term "licensee" to include, in part, "every licensed insurer, producer, and any other person licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered, under chapter 431 or 432, or holding a certificate of authority under chapter 432D."

Exempting insurance licensees from the scope of Section 3, Part II of the bill would eliminate potentially overlapping, confusing, and perhaps even inconsistent privacy provisions without reducing the privacy rights of insurance consumers in Hawaii.

The left column in the following table summarizes the key substantive elements of Section 3, Part II of the bill. The right column of the table lists several key privacy protection statutes and case law that already exist to protect consumers' right of privacy in their personal and health information or insurance regulatory statutes that prescribe retention of insurance records.

<b>HB 2572, Section 3 Part II. Consumer Rights to Personal Information</b>	<b>Existing Laws</b>
<p>§ -11 Right to request personal information; collection, disclosure, and delivery of personal information</p>	<p><i>State insurance statutes already address privacy notices to consumers. For example:</i></p> <p>HRS Chapter 431, Article 3A, Part I: general provisions</p> <p>HRS Chapter 431, Article 3A, Part II: privacy and opt out notices for financial information</p> <p>HRS Chapter 431, Article 3A, Part III: limits on disclosures of financial information</p> <p>HRS Chapter 431, Article 3A, Part IV: exceptions to limits on disclosures of financial information</p> <p><i>Other general state statutes addressing privacy issues are applicable to businesses, including insurers. For example:</i></p> <p>HRS § 487J-2 (social security number protection)</p> <p>HRS § 487J-6 (unlawful use of identification card or driver's license)</p> <p><i>Hawaii Supreme Court decisions protect consumers' state constitutional right of privacy in health information:</i></p> <p><i>Cohan v. Ayabe</i>, 132 Hawaii 408, 322 P.3d 948 (2014)</p> <p><i>Brende v. Hara</i>, 113 Hawaii 424, 153 P.2d 1109 (2007)</p>

<p>§ -12 Right to delete personal information</p> <p>(d) A business shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business to maintain the consumer's personal information to:</p> <p>(8) Comply with a legal obligation....</p>	<p><i>Current state statutes require insurers to maintain records, so consumer-requested deletions may not comply with insurers' obligations under existing insurance statutes. For example:</i></p> <p>HRS § 431:3-305 (accounts; records)</p> <p>HRS § 431:9-229 (records of adjuster or independent bill reviewer)</p> <p>HRS § 431:9A-123 (records of insurance producer)</p> <p><i>Current statute requires protection against unauthorized access to personal information records after disposal:</i> (continued)</p> <p>HRS § 487R-2 (destruction of personal information records)</p>
<p>§ -13 Discrimination against consumers</p>	<p><i>Current statute prohibits discrimination based on a consumer/customer's direction that an insurance licensee not disclose nonpublic financial information.</i></p> <p>HRS § 431:3A-502 (nondiscrimination)</p>
<p>§ -14 Obligations of a business</p>	<p><i>State insurance statute already addresses the information to be included in privacy notices:</i></p> <p>HRS § 431:3A-203 (information to be included in privacy notices)</p>
<p>§ -15 Federal law exemptions</p>	<p><i>State insurance statute does not modify, limit or supersede the federal Fair Credit Reporting Act:</i></p> <p>HRS § 431:3A-501 (protection of Fair Credit Reporting Act)</p>



§ -16 Enforcement; penalties	<i>State insurance statute includes a violation section:</i>  HRS § 431:3A-503 (violation shall be deemed an unfair method of competition or unfair or deceptive trade act or practice)
------------------------------	---

Second, the Hawaii Insurers Council requests that the definition of “personal information” in Section 3 of the bill (on page 15, line 1 through page 16, line 17) be amended to exempt from the definition information that is publicly available. The Hawaii Insurers Council recommends that the following language be inserted on page 16, after line 17:

“Personal information” does not include information that is publicly available.

Third, the definition of “publicly available” (on page 16, lines 18-21) appears to contradict the intent of the bill. The proposed definition provides, in part, that “publicly available” means “available information from federal, state, or local government records, including any conditions associated with the information.” This definition appears to include social security numbers, driver’s license numbers, passport numbers, and other similar identifiers issued by the government. The inclusion of such government-issued information in the definition of “publicly available” appears to contradict the inclusion of such information in the definition of “personal information.” In order to address this apparent contradiction, the Hawaii Insurers Council suggests the following revision to the definition of the term “publicly available”:

“Publicly available” means [available] information lawfully made available to the general public from federal, state, or local government records, including any conditions associated with the information, by the consumer, or from widely distributed media, or information that is required to be disclosed to the general public by federal, state, or local law or by court order. “Publicly available” does not include:

- (1) Biometric information collected by a business about a consumer without the consumer’s knowledge; and

- (2) Consumer information that is deidentified or aggregate consumer information.

Finally, the exemption from the definition of “personal information” in Section 2 of the bill (page 7, lines 16-19), in HRS § 487N-1, similarly should be amended as follows:

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state or local government records, including any conditions associated with the information, by the individual, or from widely distributed media, or information that is required to be disclosed to the general public by federal, state, or local law or by court order.

Thank you for the opportunity to testify.

# STATE PRIVACY AND SECURITY COALITION

---

February 25, 2020

Representative Chris Lee  
Chair, House Committee on Judiciary  
Hawaii State Capitol, Room 433  
Honolulu, HI 96813

Representative Roy Takumi  
Chair, House Committee on  
Consumer Protection and Commerce  
Hawaii State Capitol, Room 320  
Honolulu, HI 96813

**Re: HB 2572 (Oppose)**

The State Privacy & Security Coalition, a coalition of 30 leading telecommunications, technology, retail, payment card, online security, and automobile companies, as well as 8 trade associations, writes to strongly oppose HB 2572, a bill derived from the California Consumer Privacy Act (CCPA), and which also attempts to amend the state's data breach law, institute data broker reforms, regulate geolocation specifically, and regulate internet service providers. Moreover, HB 2572 contains outlier requirements that are overly prescriptive and do not reflect mainstream privacy and data security protocols.

As the state privacy landscape evolves, businesses of all sizes and consumers of varying levels of internet facility need understandable guidelines. A sixty-page piece of legislation that contains internal contradictions and will be literally impossible with which to comply will overwhelm both constituencies, costing businesses tens of millions of dollars in compliance costs, and confusing consumers.

## **I. CCPA Language**

### **CCPA is an Unfinished, Moving Target**

It does not make sense to introduce legislation in Hawaii that is based on unfinished and confusing legislation like the CCPA. Even as part of the law is now in effect, there are significant additional requirements that are still in doubt, both from 1) the interim Attorney General regulations (which have already changed twice and would add 25 pages of substantive new compliance obligations) and 2) the 2020 November Ballot Initiative, which aims to both correct errors and inconsistencies in the CCPA, and introduce additional requirements. If it passes in November, as expected, it will quickly make the existing CCPA obsolete.

Importantly, HB 2572 does not even reflect the amendments to CCPA that passed in October of 2019. These changed definitions, exempted employee information and added business-to-business regulations, and made an important change that allowed loyalty and discount programs to move forward.

## STATE PRIVACY AND SECURITY COALITION

In short, this unamended version of the CCPA, proposed by HB 2572, is so materially flawed that between last fall's amendments, as well as the AG's regulations, and the CCPA ballot initiative, this legislation will have been amended or changed eight times in the 26 months since its passage. Its ambiguities have led to the fact that since its passage in 2018, not a single state has enacted it. Neither Hawaii nor any other state should use it as a model.

Lastly, there currently three major pieces of federal privacy legislation being debated, and none of those three – proposed by Democratic and Republican members of a House Committee, a progressive Democratic Senator, and a conservative Republican Senator – use CCPA as a model or starting point, or incorporate any of its definitions.

### **CCPA Introduces Unintended, Negative Privacy Consequences**

The CCPA was passed with good intentions, but the lack of stakeholder input in the process created significant unintended consequences that incentivize anti-privacy behaviors in order to comply. HB 2572 would have the same effect.

First, HB 2572 strongly incentivizes the combination and storage of all personal information a company holds in one place to be able to comply with consumer rights requests, thereby also increasing vulnerability to hacking and fraud.

Second, because consumer data and consumer rights apply to a household as well as to an individual consumer, an abusive spouse can currently request all PI on his or her victim, and roommates can obtain financial account and social security number information about other roommates.

Third, the bill includes a fraud exemption only for the right to delete, thereby preventing a business which suspects the person submitting an access request is actually a fraudster from refusing the request. This is a data security threat and puts Hawaii consumers at serious risk of identity theft and other privacy harms.

### **CCPA Imposes Significant Compliance Costs on Business**

Not only does HB 2572 present anti-privacy consequences, it does so while imposing significant and unnecessary compliance costs on Hawaii businesses. In California, the State Department of Finance estimated that initial compliance costs for entities within the state would reach **\$55 billion**. This is not just limited to large businesses – the study estimated that approximately 75% of companies doing business in California would have to comply with the law. Businesses with 20 or fewer employees can expect to spend approximately \$50,000 to comply. For businesses with fewer than 50 employees, that number jumps to \$100,000.<sup>1</sup>

---

<sup>1</sup> [http://www.dof.ca.gov/Forecasting/Economics/Major\\_Regulations/Major\\_Regulations\\_Table/documents/CCPA\\_Regulations-SRIA-DOF.pdf](http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf)

# STATE PRIVACY AND SECURITY COALITION

## II. Data Broker Reforms

HB 2572 also proposes to institute data broker reforms. As we also point out below, it is not clear whether the CCPA language is intended to additionally apply to data brokers as well; given that the data broker law also contains consumer rights language, we assume that HB 2572 contemplates data brokers being regulated separately from any other business. However, that distinction is not made clear anywhere in the bill, and will be a compliance nightmare for businesses in the state that are not sure which regulatory scheme they will be required to abide by.

Moreover, the bill contains data security provisions that do not follow peer-reviewed and internationally accepted protocols, such as the National Institute for Standards and Technology Cybersecurity Framework, or the International Organization for Standardization (ISO) certifications. These frameworks encourage entities to evaluate their own organizations with regard to any number of cybersecurity risks, and to prioritize and tailor their solutions to the highest-level risks for their customers and employees.

Instead, HB 2572 sets forth draconian requirements that, while they may be implemented already by large entities, would be crippling to implement for small businesses (for instance, anti-fraud vendors who track suspected fraudsters and provide information to their customers). The types of data security controls that a given organization should use, and the circumstances for which they should use them, are best left to the types of international standards bodies mentioned above.

## III. Geolocation Information & Internet Browser Information

The bill also attempts to specifically legislate both geolocation information and ISP privacy. As we reference above, it is incredibly confusing to propose comprehensive legislation for all types of personal information in one way – via the CCPA language – and then segregate two particular types of data in an entirely different section of the bill.

### a. Geolocation Data

Section 4 is broad and ambiguous in a way that is likely to have unintended consequences. The Federal Trade Commission's (FTC) 2012 privacy framework notes that precise geolocation is sensitive information for which an entity should receive consent before using, and we do not oppose such a requirement. However, any bill attempting to regulate this should be carefully considered. For instance, there is no fraud exemption here, so that fraudsters could refuse to be tracked and avoid triggering red flags in systems that use location as an element that subjects suspicious transactions to closer inspection and identify patterns that help to prevent future unlawful activities.

Similarly, there is no exception for emergency services, or any health-related activities where a person is disabled and cannot provide consent, and where an entity's transfer of information to another entity (a "sale" under this bill) would mean the literal difference between life and death.

## STATE PRIVACY AND SECURITY COALITION

These problems will likely ensue due to the use of the CCPA definition of “sale” – a definition which is at the heart of most of CCPA’s unintended consequences. Using this definition in this context will almost surely cause similar unintended consequences. For example, if a consumer requests a transaction that involves the disclosure of location information from a business to its service provider, must the consumer provide express consent to do so? What if the consumer requests such a transaction but does not provide the consent necessary to complete the transaction?

HB 2572 is also broad enough to include every photograph or video that is captured by a phone and transferred by a photo application to a cloud storage company. It could also include any information that contains a consumer’s zip code, which would provide some broad sense of a consumer’s location; or information that contains a customer’s purchase history but does not include geolocation information. These types of unintended consequence should be avoided.

Of course, Hawaii is a unique and treasured tourist destination. The Hawaii Tourism Authority estimated that in 2017, 9.3 million tourists visited. If every tourist took even 5 photos, that would be 46.5 million photos generated. Subjecting each one of these to enforcement as a result of, for example, a consumer transferring a photograph from a consumer’s email account to his or her social media account is likely not what the legislature intends to regulate, but applying the CCPA’s definition of “sale,” that is exactly what would occur.

### **b. Internet Browser Information**

The latter part of section 4 departs from the FTC’s Privacy Framework, because browsing history is not considered sensitive information, and because different segments of such information are frequently transferred to keep the provision of services free, as well as to detect suspicious and fraudulent activity that harms individuals conducting legitimate online activity.

This provision also creates inconsistencies with the CCPA definition of “personal information” earlier in the bill, which explicitly includes internet browsing activity and internet protocol addresses. Of course, the CCPA does not require opt-in consent to collect or use these types of information, meaning that a business is permitted to transfer this information to another entity under one provision of HB 2572, but prohibited from doing so without consent under a different provision of the same bill.

Similar to the problems created by using the CCPA definition of “sale” with geolocation information, using the definition of “sale” here fails to recognize the modern online ecosystem. The bill would impose unreasonable and unwarranted obligations before an internet service provider or any other entity could perform functions that are likely well within the consumer’s expectations.

If consumers do not opt in to uses of data that permit companies to develop new products and services, or to certain sharing of cybersecurity threat information, both businesses and consumers will suffer. Similarly, much of the free news and content that is available online is supported by

## STATE PRIVACY AND SECURITY COALITION

advertising, which takes place through the exchange of pseudonymous identifiers. This presents little risk to individuals, who may already opt out of the use of their data for most advertising purposes.<sup>2</sup> Requiring consumers to opt in to these low-risk uses of information that characterize the flow of online services is likely to impact these free services that consumers have come to enjoy.

In conclusion, HB 2572 is a sprawling piece of legislation that will be nearly impossible to comply with and impossible for both businesses and consumers to understand. We would be willing to work with your committees on a better alternative that achieves the same comprehensive goals but is much simpler and provides more meaningful consumer benefits.

Respectfully submitted,



Andrew Kingman  
General Counsel  
State Privacy and Security Coalition

---

<sup>2</sup> See, e.g., Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 40-44 (2012); CAN-SPAM CITE; Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at: <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; Network Advertising Initiative Code of Conduct (2018), available at: [http://www.networkadvertising.org/sites/default/files/nai\\_code2018.pdf](http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf).



Charter Communications  
Testimony of Myoung Oh, Director of Government Affairs

**COMMITTEE ON JUDICIARY**

**COMMITTEE ON CONSUMER PROTECTION AND COMMERCE**

Hawai'i State Capitol, Conference Room 329  
Tuesday, February 25, 2020  
3:00 PM

**WRITTEN COMMENTS AND CONCERNS ON H.B. 2572, H.D.1 , RELATING TO PRIVACY**

Chair Lee , Chair Takumi, Vice-Chair San Buenaventura, Vice-Chair Ichiyama and Members of the Joint Committees.

Charter Communications, Inc. ("Charter") is pleased to have this opportunity to provide its views on H.B. 2572, H.D.1. As explained below, Charter supports Hawaii's efforts to protect the privacy of consumer personal data, and looks forward to working with these Committees and other stakeholders to achieve that goal, but opposes enactment of the bill in its current form.

As the largest broadband provider in Hawai'i with services available to over 400,000 homes and businesses in all 4 Counties, including Molokai and Lanai, Charter Communications is committed to providing customers with superior products and services. As a result of significant network investments, Charter's base broadband speed is 200/10Mbps and we now offer Spectrum Internet Gig (with download speeds of 940 Mbps) in almost all of Hawai'i. Charter continues to significantly invest in and provide infrastructure improvements, unleashing the power of an advanced, two-way, fully interactive fiber network. By moving to an all-digital network, today's Spectrum customers enjoy



more HD channels, more On Demand offerings, more video choices than ever before, and the fastest internet speeds and the most consistent performance available. Charter offers these services without data caps, modem fees, annual contracts, or early termination fees.

An increasingly important aspect of ensuring that consumers continue to utilize all the services the internet has to offer is making sure they are confident that their personal information is protected. Charter enthusiastically supports such protections, and has taken an active role in promoting potential approaches to address the complex issues that impact consumers' online privacy. As Charter has expressed in testimony before Congress and in state houses across the country, an effective privacy framework must be based primarily on five principles.

The first principle is control. Consumers should be empowered to have meaningful choice regarding the collection and use of their data. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear, and meaningful. Additionally, consent should be renewed with reasonable frequency, and any use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. We recognize that there are several policy options as to how to provide consumers with control of their information, and we are willing to work with stakeholders to find practical and impactful solutions.

The second principle is transparency. Consumers should be given the information they need to provide informed consent. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand, and readily available.

The third principle is parity. Consumers are best served by a uniform framework that is applied consistently across the entire internet ecosystem, not based on who is collecting it or what type of service is being offered. Consumers' data should be protected equally whether they are using an ISP, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device.

The fourth principle is uniformity. We believe that for online consumer protections to be effective there should be a single national standard. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation. However, we realize that in the absence of a uniform, federal solution, some states may consider acting on their own. In doing so, it will be critical that the states understand what each of the others is doing so as to avoid an inconsistent or worse, contradictory, set of online protections.

The final principle is security. We believe privacy is security and security is privacy. Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

### **CONCERNS WITH HB 2572**

H.B. 2572, H.D.1 addresses several, distinct, privacy-related issues within a single bill. Among the issues addressed are data brokers, government access to data, deepfakes, data breach notification, and several consumer rights in Parts III and IV. The consumer rights addressed in this bill relate to transparency, nondiscrimination, data access, data deletion, and opt-in to sales of geolocation and

internet browser information. Though each of these are important issues, and Charter hopes to work with Hawai'i to address each of them, this testimony focuses primarily on our concerns with how the consumer rights provided for in Parts III and IV of the bill are structured and offers improvements to the language to address these concerns.

In its current form, the manner in which H.B. 2572, H.D.1 addresses these consumer rights is significantly flawed. While these provisions appear to be based in large part on the California Consumer Privacy Act of 2018 (the "CCPA"), H.B. 2572, H.D.1 omits a number of critical amendments made to the California law in 2019 to clarify the initially-enacted version of that law. For instance, the 2019 CCPA amendments made important changes to the definition of "personal information", and recognized that certain online businesses should not be required to provide toll free telephone numbers as a means of consumers exercising their privacy rights. Without these amendments, the consumer rights provisions of H.B. 2572, H.D.1 ignore the improvements that California recognized were necessary to its privacy framework.

Even if H.B. 2572, H.D.1 were to be amended to address the missing 2019 CCPA amendments, we would urge the Committees to not rely on the CCPA as a model for privacy legislation, as that law is still very much a work-in-progress. Even though the CCPA went into effect on January 1, 2020, there are significant additional requirements under the CCPA that are in doubt. Indeed, the California Attorney General has not yet finalized any of the required CCPA regulations. Just as recently as February 7, 2020, the California Attorney General released modifications to the proposed CCPA regulations, which triggered a further public comment period to February 25, 2020. At this juncture,

it would seem highly unlikely that the CCPA regulations would be issued before the end of the first quarter of this year. That means the CCPA will have been in effect for months before any of the required regulations – some of which would impose significant additional burdens on companies beyond the statutory text of the CCPA – have been finalized.

And while companies are left to wait to see what the final requirements of the existing CCPA will be, there is a November 2020 ballot initiative in California that would significantly amend the still unsettled CCPA. If passed, companies will have spent years preparing for a statutory regime that will then only have been in effect for a handful of months before being changed dramatically again. Given the ballot initiative, the Attorney General's pending regulations, and provisions of the existing CCPA that sunset after 2020, it is exceedingly likely that the CCPA as we know it today will look very different next year. In light of the fluid state of the CCPA regime, it should not form the basis for a comprehensive privacy bill in Hawai'i.

Additionally, the CCPA has also already shown itself to have unintended negative consequences for businesses and consumers. One of the byproducts of the breadth of the consumer rights granted under the CCPA is that businesses are strongly incentivized to combine the storage of all consumer personal information in one place in order to respond to consumer requests to know, access, or delete information. Storing all personal data in one location significantly increases the vulnerability of that data to a cyberattack or fraudster. Another unintended consequence is that because consumer rights were granted to "households" in addition to individuals, the CCPA in its current form may inadvertently permit an abusive spouse to request the personal information of all

of his or her victims in the same household. And because of that definition, roommates sharing the same video or broadband subscription can obtain financial account and other sensitive information about each other. While these issues may be addressed in the California Attorney General's regulations, as discussed above, those are not yet final, and regardless are not yet reflected in the text of the CCPA on which H.B. 2572, H.D.1 is modeled.

Compounding the issues of using an outdated version of CCPA as a model is the fact that H.B. 2572, H.D.1 does so inconsistently. By cherry-picking parts of the CCPA even within the specific rights outlined in that law to form the basis for H.B. 2572, H.D.1's consumer rights provisions, H.B. 2572, H.D.1 fails to give consideration to the careful balancing that went into defining the extent of those rights in the CCPA as well as to the critical clarifications that exist in omitted portions of those rights as defined by the CCPA.

Moreover, nothing in the Twenty-first Century Privacy Law Task Force (the "Task Force") report gives any indication that the language ultimately proposed in the consumer rights provisions in Parts III and IV of H.B. 2572, H.D.1 was considered by that group. Charter Communications participated in the Task Force, and whether to import these parts of California's privacy model was not part of the discussion. In California as well as other states that are determining whether omnibus privacy legislation is right for them, there has been a robust and meaningful stakeholder process to solicit different views and opinions on each of the different privacy rights and the statutory language that will best provide for those consumer rights. That has not occurred here with respect to the consumer rights language pulled from the CCPA into Parts III and IV of H.B. 2572, H.D.1. While Charter

supports granting consumers the rights provided for in these provisions, we encourage the legislature to take the additional time necessary to fully consider the best approach to doing so.

There are, however, other parts of H.B. 2572, H.D.1 that, with some work, could be reasonable places to start the process of updating privacy protections in Hawai'i. Unlike the consumer rights provisions, there are more settled models on which to rely with respect to data breach notification and government access to data. For example, with respect to Part II of H.B. 2572, H.D.1, the modifications represent an over correction to HRS 487N-1, and would place Hawaii's law in conflict with literally every other state and U.S. territory data breach notification law. The amendments proposed to HRS 487N-1 would do away with the encryption safe harbor, which for good reason is in every other state and territory's data breach law; encryption could eliminate the risk of harm even in the event of a breach, and so should be encouraged by the law.

## **CONCLUSION**

Charter is committed to ensuring that consumer information is protected across the internet ecosystem. That is why, two years ago, our CEO broke new ground by calling for the enactment of federal legislation mandating that all companies receive affirmative, opt-in consent before collecting or sharing their customers' data. And since that time, Charter representatives have appeared voluntarily and on numerous occasions before lawmakers and policymakers—including Congress and the Federal Trade Commission—to support such a federal privacy law.

While parts of H.B. 2572, H.D.1 reflect positive steps forward, the consumer rights provisions of the bill in its existing form would create more problems for businesses and consumers than they

would solve. Charter looks forward to working with Members of the Committees, industry partners, consumer groups, and other stakeholders in this process to address the privacy of our consumers holistically, sensibly, and effectively through more deliberate legislation.

Thank you again for the opportunity for Charter to present its views.



February 24, 2020

The Honorable Chris Lee, Chair  
The Honorable Joy A. San Buenaventura, Vice Chair  
House Committee on Judiciary

The Honorable Roy M. Takumi, Chair  
The Honorable Linda Ichiyama, Vice Chair  
House Committee on Consumer Protection & Commerce

Re: HB 2572 HD1 – Relating to Privacy

Dear Chair Lee, Chair Takumi, Vice Chair San Buenaventura, Vice Chair Ichiyama, and Members of the Committees:

The Hawaii Medical Service Association (HMSA) appreciates the opportunity to testify on HB 2572, HD1, which redefines "personal information" for the purposes of security breach of personal information law. Establishes new provisions on consumer rights to personal information and data brokers. Prohibits the sale of geolocation information and internet browser information without consent. Amends provisions relating to electronic eavesdropping law. Prohibits certain manipulated images of individuals.

HMSA supports the intent of this measure to protect personal information of consumers. We appreciate the exemption in Part II of the bill for covered entities governed by or otherwise subject to the federal Health Insurance Portability and Availability Act of 1996 (HIPAA). California provided the same exemption in its California Consumer Privacy Act of 2018, but also included business associates of covered entities as well. We respectfully ask that this exemption also apply to a "business associate" of a covered entity as defined in HIPAA. We also respectfully ask that this exemption apply to all parts of the bill and not just Part II.

Thank you for the opportunity to provide testimony on this measure.

Sincerely,

Jennifer Diesman  
Senior Vice President Government Relations





To: The Honorable Representative Chris Lee, Chair  
The Honorable Representative Joy A. San Buenaventura, Vice Chair  
House Committee on Judiciary

The Honorable Representative Roy M. Takumi, Chair  
The Honorable Representative Linda Ichiyama, Vice Chair  
House Committee on Consumer Protection and Commerce

From: Mark Sektnan, Vice President

Re: **HB 2572 HD1 Relating to Privacy**  
**APCIA Position: OPPOSE**

Date: Tuesday, February 25, 2020  
3:00 p.m., Room 329

Aloha Chairs Lee and Takumi, Vice Chairs San Buenaventura and Ichiyama and Members of the Committees:

The American Property Casualty Insurance Association of America (APCIA) is opposed to HB 2572 HD1 which restricts the collection of personal information by businesses. Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

Consumer privacy and data security are priority issues for the insurance industry and insurers devote considerable resources to protect data, information systems, and consumer trust. As financial institutions, insurers are subject to the Gramm Leach Bliley Act (GLBA). In addition, all 50 states and the District of Columbia have adopted insurance regulations implementing GLBA and/or have statutes consistent with and, in some instances, stricter than GLBA. Specifically, Hawaii has existing law in the Insurance Code to protect the privacy of insurer consumers. Further, insurers are subject to financial and market regulation by the Hawaii Department of Insurance. As such, the current privacy framework for insurers is built on a strong and robust framework that has evolved to meet consumer expectations.

HB 2572 HD1 raises significant concerns regarding unnecessary obstacles and potential unintended consequences that will overturn this long-established privacy framework. Not only will insurers be forced to balance how to effectively manage differing obligations, but they will also be subject to dual enforcement. Included below are additional non-exhaustive substantive

concerns with HB 2572 HD1 to further support our opposition and the need for an entity-based insurance exemption.

The bill appears to be modeled after the California Consumer Protection Act (CCPA). It should be noted that the CCPA is still being amended and the regulations, which were required be adopted by January 1, 2020 are still being developed. HB 2572 HD1 also contains some different elements including, but not limited to the following:

- Page 18 – 20: Like the CCPA, it includes a right to request personal information (PI) held by a business and requires notice at the time of collection as to what personal information will be collected and how it will be used. Additional uses will require additional disclosures prior to use.
- Page 21 - 23: Gives consumers the right to demand deletion of PI that a business has collected from the consumer.
- There are various exceptions to the foregoing, but subsection (6) on p. 28, lines 11+ contains an exception to the exception that creates some possible confusion. It states that the provisions don't restrict a business's ability to collect or sell PI if the business collected it while the consumer was out of state, except that it doesn't authorize the business to store PI when the consumer is in the state. This is contradictory. That provision also attempts to reach beyond the state, by prohibiting the subsequent collection of PI when the consumer is outside the state. This seems unenforceable.
- PI that is protected by HIPAA, FCRA and GLBA is exempt. Missing from the list is PI protected by the Driver's Privacy Protection Act (DPPA), PI associated with business-to-business transactions, and PI collected and used for employment/contractor purposes. These should be added as exemptions.
- Page 30, lines 3 – 5 set out a statutory fine of \$7,500/offense. Given the potential volume of transactions, this is very high. In fact, this is the amount for intentional violations under the CCPA with \$2,500 being the norm.
- Page 30, Part III, regulates data brokers. There are concerns if the definition is broadened to include the company, there are concerns about the prescriptive nature of the security requirements. Rather than specify specific types of security measures, the better approach would be to allow entities to design their security based on their risk assessments.
- Page 46, lines 11 + restrict the sale of internet browser information without consent. This will be very problematic as it will interfere with online advertising and tracking the effectiveness of the advertising. It will be nearly impossible to obtain consent for this activity, impairing the effectiveness of our advertising and ability to measure it. By contrast, the CCPA allows consumers to opt out of this activity, unless it is comprised of an exchange with a "service provider," which is an entity that processes data for a business with the promise that it will not be used for other purposes not recognized as legitimate by the CCPA. This is a key element of CCPA that should be included here.
- Page 59, line 16: States that the act will take effect upon approval. Businesses will require time to comply. A year would not be too long.

For these reasons, APCIA asks that this bill be held in committee.

Representative Chris Lee  
Chair, House Committee on Judiciary  
Hawaii State Capitol, Room 433  
Honolulu, HI 96813

Representative Roy Takumi  
Chair, House Committee on  
Consumer Protection and Commerce  
Hawaii State Capitol, Room 320  
Honolulu, HI 96813

**Re: HB 2572, HD 1 (Oppose)**

On behalf of RELX, a world-leading provider of technology solutions that support the government, insurance, and financial services industries in making communities safer, insurance rates more accurate, commerce more transparent, and processes more efficient, we write to raise concerns with House Bill 2572, HD 1 as currently drafted.

Given the complex and interconnected data ecosystems that support consumers, it cannot be overstated how important it is to take a thoughtful and informed approach to drafting legislation that provides both consumers and industry with a workable framework to enhance data privacy protections.

We are concerned with a patchwork approach that seeks to impose different privacy and security obligations on different types of businesses while the underlying data remains the same. It is our hope that legislators of Hawaii will legislate in a way that avoids creating a confusing, unworkable and unfair privacy regime, and that you will work with industry on an alternate approach that preserves consumer trust and confidence, while supporting flexibility in the flow of information.

Specifically, to ensure that the rights of consumers are protected while also allowing for the appropriate and responsible use of data without creating negative unintended consequences, additional changes are needed as outlined below.

**1. Data privacy obligations to protect consumers should be triggered by the nature and use of the data, not by an arbitrary business model designation.**

No one disputes that businesses should be good stewards of consumer information and ensure responsible and secure use of data. However, granting preferential treatment under the law based on one business model when the underlying need to protect and secure consumer information is universal is not appropriate. The legislation should not create a dual and uneven regulatory regime based on an artificial and limited definition of data brokers and other businesses. This legislation makes the mistake of focusing on the status of the holder of the data, and not the kind of data being held or used by the business. In all instances the importance of protecting consumer information is the same and thus obligations imposed by the bill should be equally applied.

## **2. Specific exemptions are needed for data regulated by federal privacy laws.**

To avoid dual and potentially conflicting regulatory obligations, privacy legislation must include consideration of preexisting federal privacy laws including the 1.) The Fair Credit Reporting Act (FCRA), 15 USC 1681, 1681b; 2.) The Gramm Leach Bliley Act (GLBA), 15 USC 6801, 6802(e); 3.) The Driver's Privacy Protection Act (DPPA), 18 USC 2721, 2721(b); 4.) The Health Information Portability and Accountability Act (HIPAA), Public Law 104-191; and 5.) The Health Information Technology for Economic and Clinical Health Act (HITECH), Public Law 111-5. These laws ensure that personally identifiable data can only be used for specific purposes set forth in the various governing statutes.

The FCRA and DPPA, as with GLBA, HIPAA, and HITECH, provide long-standing and robust protections for consumers. These statutes are enforced by various agencies including the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) in the case of FCRA and GLBA, the Department of Health and Human Services (HHS) in the case of HIPAA and HITECH, and the Department of Justice (DOJ) and state departments of motor vehicles in the case of DPPA.

## **3. First Amendment protection of public records must be recognized.**

There are important interests rooted in the First Amendment to the U.S. Constitution supporting the free use of publicly available information. If information is lawfully made available to the public and subsequently lawfully obtained by a third party, the restriction of such third party's use of such information raises significant free speech concerns such as: imposing a burden on speech without advancing a compelling or substantial government interest for doing so, vague standards, and discriminating against types of speakers by limiting the use of public records by controllers and processors but not others.

From a practical standpoint, it is worth noting that government agencies tend to rely heavily upon bulk public records data provided from private vendors to assist in their core missions. For example, a foster youth agency may obtain tax records to find biological relatives of foster children or a child support enforcement agency may use a marriage license or criminal record to locate a non-custodial parent. We believe that publicly available records should be exempt across all provisions included in the legislation to avoid a patchwork problem of various conflicting state laws.

## **4. To further protect consumers and help prevent identity theft, an exemption should be included for data that is collected and used to prevent fraud or to meet compliance obligations under applicable federal, state, and local laws.**

Without a clear fraud exception, privacy rights can be subverted by bad actors and identity thieves to receive disclosures of sensitive information or restrict processing of individual data intended to protect the consumer. Without proper protections in place, bad actors will have an easier time fraudulently using a consumer's identity to obtain goods and services. By requesting deletion of a consumer's information, bad actors may prevent merchants from relying upon

commercially provided identity verification tools to confirm that the purchaser is who they say they are.

### **Conclusion**

We sincerely appreciate your consideration of the feedback provided and would like to direct your attention to the California Consumer Privacy Act as amended in the 2019 legislative session, as well as the Washington Privacy Act as passed by the Washington State Senate earlier this month on a bipartisan vote of 46-1. Both pieces of legislation received broad stakeholder input and would address many of the concerns we have raised in our comments.

We look forward to working with you as this effort continues and offer the expertise of our privacy counsel should you have any questions or require additional materials. Please feel free to contact me at 202-716-7867 or at [london.biggs@relx.com](mailto:london.biggs@relx.com) if I can be of further assistance.

Sincerely,

*London Biggs*, Senior Manager, State Government Affairs - West  
RELX Inc.



February 24<sup>th</sup>, 2020

Representative Chris Lee  
Chair, House Committee on Judiciary

Representative Roy Takumi  
Chair, House Committee on  
Consumer Protection and Commerce

**Re: CompTIA Opposes HB 2572**

Dear Chair Lee and Chair Takumi,

CompTIA, or the Computing Technology Industry Association, represents the country's leading technology firms. We write to you today in opposition to House Bill 2572 and ask that you please keep this bill from passing out of your committee.

Consumer protection is the number one priority for our members. Earning a consumer's trust simply makes for good business. While CompTIA strongly believes that the best consumer privacy framework for both business and consumers is a framework created at the federal level, some individual states feel the urge to act now. However, Hawaii HB 2572 is a sweeping legislation that, among other things, would make it impossible for companies to comply with and only confuse consumers.

House Bill 2572 is based on the California Consumer Privacy Act (CCPA), legislation that has taken years to draft and continues to be amended and reworked. The process in California has lacked input from technology companies, which makes the bill more difficult to comply with as it may not align with industry practices. The Hawaii Legislature should seek the best privacy legislation for its consumers, a goal shared by our members. Moving forward with a bill that is unfinished and lacks industry input for optimal compliance will only make it more difficult for consumers to understand their rights.

Furthermore, HB 2572 incorporates language from other statutes, such as the Vermont data broker law and geolocation bills. Passing data privacy legislation is complicated enough but trying to incorporate other aspects of privacy legislation into a single bill will create more confusion and barriers to companies to who want to comply.

CompTIA would be willing to work with your committees to draft workable legislation that provides better protections for consumers and allows for better industry compliance. Please keep HB 2572 from moving forward and allow industry to engage in a robust stakeholder conversation to create better privacy legislation for Hawaii.

Sincerely,

Anna Powell  
Director, State Government Affairs - West



**Hawaiian  
Electric**

**TESTIMONY BEFORE THE HOUSE COMMITTEES ON  
JUDICIARY  
&  
CONSUMER PROTECTION AND COMMERCE**

**H.B. 2572, HD1**

**Relating to Privacy**

Tuesday, February 25, 2020

3:00 p.m.

State Capitol, Conference Room 329

Wendee Hilderbrand  
Managing Counsel & Privacy Officer  
Hawaiian Electric Company, Inc.

Dear Chair Lee and Chair Takumi, Vice Chair San Buenaventura and Vice Chair Ichiyama, and Committee Members,

My name is Wendee Hilderbrand, and I am testifying on behalf of Hawaiian Electric Company, Inc. (Hawaiian Electric) **in opposition to H.B. 2572, HD1**. While Hawaiian Electric is generally supportive of modernizing Hawaii's privacy laws, providing increased protection of consumer information, and providing consumers increased rights with regard to their information, it is important that we do so in a way that balances the benefit to consumers with the costs that will necessarily be passed through to them. As written, H.B. 2572, HD1 is unnecessarily broad and would lead to significant unintended consequences.

Hawaiian Electric has already implemented an extremely consumer-friendly privacy policy. Our Company does not use consumer information outside of the ordinary needs of our business, unless acting upon the written consent of the consumer or an order from the State of Hawaii Public Utility Commission or other legal authority.

We do not buy consumer information, nor do we sell consumer information. Hawaiian Electric voluntarily complies with the heightened DataGuard standards recommended by the Department of Energy and has never come under regulatory scrutiny for its consumer privacy practices.

Thus, while Hawaiian Electric is generally not opposed to adding a Consumer Privacy chapter to title 26 of the Hawaii Revised Statutes (H.R.S.), Part III of H.B. 2572, HD1 is taken almost verbatim from a bill that passed in California and has already proven to be extremely expensive and difficult for businesses to comply with. Indeed, after its initial passage, California has had to amend its legislation to address the overbreadth of the initial bill; between passage and implementation, 19 amendments were proposed, 7 of which were adopted. Inexplicably, the most important amendment – which exempts employer-employee data – was not included in H.B. 2572, HD1, making the proposed Hawaii bill even broader than the troublesome California bill.

To address extreme cases where consumer data is bought and sold as a commodity, H.B. 2572, HD1 takes a blanket approach to all businesses, regardless of purpose, and virtually every type of data collected. If adopted, Hawaiian Electric would have to reconfigure its record-keeping systems so all records (including call recordings, surveillance tapes, meter readings, maintenance records, outage notices, payment records, service applications, equipment complaints, etc.) were searchable by the names of Hawaii residents to enable collection and production upon request. There are no exceptions to the obligation to produce a record when, for example, it contains confidential details about Company processes or personnel, information about another customer, or supervisor impressions about an employee. Moreover, the bill gives individuals the right to demand that Hawaiian Electric delete all information about them



unless certain exceptions apply. There seems to be nothing in the exceptions to prevent, for example, a former employee from demanding deletion of her employment file; a former customer from demanding deletion of his past payment records; or a non-customer from demanding deletion of call recordings the Company made when she called and threatened one of our employees.

These are just some of the concerns Hawaiian Electric has with Part III of H.B. 2572, HD1, as broadly as it is currently written. If it were limited to businesses that trade in customer information, very broad protections and rights may be necessary. However, if the desire is to provide all Hawaii residents (whether acting as customers, employees, or neither of the above) with protections from and rights vis a vis all businesses (whether data brokers, car dealerships, or public utilities), respectfully, more thought needs to be given to the scope in order to avoid unintended consequences to Hawaii's businesses and significant cost pass-through to Hawaii's residents.

Hawaiian Electric's concerns with Part II of H.B. 2572, HD1 may be addressable by amendment. The Company agrees that the statutory definition of personal information in H.R.S. 487N-1 is in need of updating; however, Hawaiian Electric requests that Part II, Section 2, 1. be amended to clarify the intent of subparagraph (5) and to delete subparagraphs (6) and (7). Currently, H.R.S. 487N-1 protects financial account numbers, as well as passcodes that "would permit access to an individual's financial account." *Id.* at (3). The proposed bill would separate financial accounts from passcodes, but in doing so, does not limit protected passcodes to those that can be used to access a financial account. So, for example, the passcode to a Netflix account would receive the same protection as the passcode to a bank account, and in fact, the passcode to a non-financial account (e.g., a utility account) would receive greater

protection than the actual account number. There is no indication in the Twenty-First Century Privacy Law Task Force Report to the Legislature (“Task Force Report”) that this change was intended, so it may be addressed by a simple amendment to Part II, Section 2, 1. (5).

Finally, H.B. 2572, HD1 proposes to add health information to the categories of information that are considered protected personal information. See Part II, Section 2, 1. (6) & (7). Health information, however, is already heavily regulated by federal statute under the Health Insurance Portability and Accountability Act (“HIPAA”) and its associated regulations. Over the last 25 years, the federal government has engaged in a delicate balancing act between protecting personal health information and facilitating the reasonable needs of businesses. If health information were added to H.R.S. § 487N-1, Hawaii businesses would be subject to conflicting requirements under federal and state law. Unlike HIPAA, H.B. 2572, HD1 has not accounted for legitimate business needs such as the use of health information in the context of worker’s compensation cases, health emergencies, law enforcement investigations, and business licensing and regulation. These issues seem unnecessary given that HIPAA already protects the privacy of health information, whereas H.R.S. § 487N-1 is aimed at preventing identity theft, which is generally not perpetrated with health information. These additions were also not explained in the Task Force Report, so again, these concerns may be addressed by deletion of Part II, Section 2, 1. (6) & (7).

Accordingly, the Hawaiian Electric Companies oppose H.B. 2572, HD1, as written. Thank you for this opportunity to testify.

Presentation to The  
Committee on Judiciary  
Committee on Consumer Protection & Commerce  
February 25, 2020 3:00 p.m.  
State Capitol Conference Room 329

**Testimony on HB 2572, HD 1 in Opposition**

TO: The Honorable Chris Lee, Chair  
The Honorable Roy M. Takumi, Chair  
The Honorable Joy A. San Buenaventura,  
The Honorable Linda Ichiyama, Vice Chair  
Members of the Committees

My name is Neal K. Okabayashi, the Executive Director of the Hawaii Bankers Association (HBA). HBA is the trade association representing eight Hawaii banks and two banks from the continent with branches in Hawaii.

HBA does not object to the concept of privacy, and in fact, the American Bankers Association testified on December 4, 2019 before a Senate Committee on the ABA's support for a national privacy and data protection measures.

Certainly, it is a difficult task to balance strong consumer protections and the need for consumer financial transactions in a safe environment, and not hampering innovation that inures to the benefit of consumers.

The difficulty of that task is evidenced by the California experience when passing the California Consumer Privacy Act (CCPA) which HB 2572 is modeled after. In fact, as soon as the bill was enacted into law on June 18, 2018, a bill was introduced to amend CCPA, which bill to amend CCPA was enacted on August 31, 2018. There have been at least six bills amending the CCPA. The lesson is that though this is a worthwhile cause, it is also a complex and complicated issue which requires great thought, examination, and wordsmithing rather than any rush to judgment.

The complexity of the bill is reflected in that our members are still working diligently to wrap their arms around the complexity of this bill. However, we wish to suggest some changes which would ameliorate some, but not all, of the flaws in the bill.

One example of the amendments is the exemption language in the bill on page 29, starting on line 19. That exemption language in HB 2572, HD 1, was in the original CCPA but was immediately amended as all recognized the language was unworkable.

The Gramm-Leach Bliley Act (GLB) exemption was one of the first provisions in CCPA that quickly fell by the wayside after being amended on August 31, 2018, less than three months after enactment of CCPA on June 18, 2018.

We propose that the following language be substituted in lieu of the current language in part II. Section 15(c):

“(c) For a non-bank or savings association financial institution who is subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), this part shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act and implementing regulations. Provided further that this part shall not apply to a banks or savings association, as defined in 12 United States Code section 1813, the deposits of which are insured by the Federal Deposit Insurance Corporation, and who are subject to Regulation P, as time to time amended by the Consumer Financial Protection Bureau or successor department, agency, or bureau, and which bank or savings association’s primary supervisory authority is the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, or the Office of the Comptroller of the Currency. “

Although banks and savings associations (banks) are not the only entities subject to GLB, banks are subject to robust and thorough examinations by bank regulatory bodies, which examinations covers compliance, including compliance with privacy laws and Regulation P, and information technology; all of which is an added layer of protection for consumers. The bank regulatory agencies do not need to await a violation before acting to thwart a potential privacy misstep.

Banks are subject to comprehensive oversight of IT technology as a protective measure against cybersecurity intrusions which may impact privacy. Federal Reserve Chair Jay Powell recently told Congress that cybersecurity is a risk for banks and other bank regulators have cited cybersecurity as a grave risk.

Reg P is a privacy regulation under the control of the Consumer Financial Protection Bureau, which controls any future amendments thereof. The three banking regulatory agencies have incorporated Reg P into its own regulations. There are other federal privacy statutes such as the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act. The FCRA exemption language will be addressed by the Consumer Data Industry Association and HBA supports their proposal on the FCRA.

The banking agencies are also allowed to impose severe penalties for unsafe and unsound practices and privacy violations could be an unsafe and unsound practice.

The consumers’ privacy concerns are well protected by Regulation P and the bank regulatory agencies, and therefore worthy of the proposed exemption.

There are other definitional items that require changes to protect the public.

The definition of “business” should be amended as follows, to be consistent with the CCPA:

“(c) “Business” means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in this state, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars (\$25,000,000), as adjusted in April of every odd-numbered year to reflect any increase to reflect any increase in the Consumer Price Index for all Urban Consumers CPI\_U) for Honolulu, and the amount of the increase shall be determined by the Hawaii Department of Business, Economic Development & Tourism,

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices,

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

For purposes of part II and part III, an entity that is organized under Internal Revenue Sections 501(c)(3) or 501(c)(6) is not a business.”

The last sentence is not part of CCPA, but non-profits are usually organized under sections 501(c)(3) or 501(c)(6).

As presently drafted, any mom and pop store, a church, a condominium association, or an educational institution would be deemed to be a “business” subject to this privacy bill. To protect small entities, many of which are individuals and consumers, this amendment is needed. The three thresholds are derived from the CCPA and protects the little guy. California did a preliminary estimate that the cost of complying with the CCPA over a ten-year period would range from \$467 million to \$16.454 billion, which estimate emphasizes the compliance cost.

The definition of consumer on page 12, line 1, should be amended by substituting the following language:

“Consumer means a natural person residing in the state who obtains a product or service primarily for personal, family, or household purpose.”

This language is consistent with the GLB, the Truth-In-Lending Act, and HRS section 480-1, and most statutory definitions of consumer. As presently drafted, a consumer can be an employee (I understand California is considering an amendment to correct the definition as a result) and more importantly a businessperson since an individual could be a solo proprietor acting in a capacity of a businessperson. The current definition could also impact B2B or P2P transactions.

To be consistent with the CCPA, the definition of “personal information” on page 15, line 1, should be amended by inserting “reasonably” on line 2, before the word “capable”. Following clause (11) on page 16, line 17, the following amendment should be included for clarity:

“Personal information does not include the following:

(1) publicly available information,

(2) consumer information that is deidentified or aggregate consumer information.”

The foregoing language is consistent with the CCPA.

We are reviewing whether further amendments to “personal information” are required.

We are reviewing the definition of “sell” on page 17, starting on line 5, since it differs in detail from CCAP. One possible amendment is to include language on when a transaction is not a sale of personal information.

We are also reviewing the part of data brokers since, to my knowledge, Vermont is the only state to have enacted a law on data brokers and that law only became effective on January 1, 2019 and thus there is little history, if at all, to guide us on the merits of the law.

Because of the complexity of compliance if the bill becomes law, the effective date should be July 1, 2022.

We thank you for this opportunity to partially inform you of HBA’s issues with certain parts of this bill. However, we will have additional comments and suggestions as we get a better handle of this bill.

Thank you for the opportunity to submit this testimony to offer our opposition on HB 2572, HD 1. Please let us know if we can provide further information.

Neal K. Okabayashi  
(808) 524-5161

# HAWAII FINANCIAL SERVICES ASSOCIATION

c/o Marvin S.C. Dang, Attorney-at-Law

P.O. Box 4109

Honolulu, Hawaii 96812-4109

Telephone No.: (808) 521-8521

February 25, 2020

Rep. Chris Lee, Chair, and Rep. Joy A. San Buenaventura, Vice Chair  
and members of the House Committee on Judiciary  
Rep. Roy M. Takumi, Chair, and Rep. Linda Ichiyama, Vice Chair  
and members of the House Committee on Consumer Protection & Commerce  
Hawaii State Capitol  
Honolulu, Hawaii 96813

Re: **H.B. 2572, H.D. 1 (Privacy)**  
**Hearing Date/Time: Tuesday, February 25, 2020, 3:00 p.m.**

I am Marvin Dang, the attorney for the **Hawaii Financial Services Association** (“HFSA”). The HFSA is a trade association for Hawaii’s consumer credit industry. Its members include Hawaii financial services loan companies (which make mortgage loans and other loans, and which are regulated by the Hawaii Commissioner of Financial Institutions), mortgage lenders, and financial institutions.

**The HFSA opposes this Bill as drafted, and we propose amendments.**

This Bill does the following: (1) redefines “personal information” for the purposes of security breach of personal information law; (2) establishes new provisions on consumer rights to personal information and data brokers; (3) prohibits the sale of geolocation information and internet browser information without consent; (4) amends provisions relating to electronic eavesdropping law; and (5) prohibits certain manipulated images of individuals.

Much of this Bill is modeled on the California Consumer Privacy Act (“CCPA”). In the course of a 7 day period in 2018, CCPA was hastily drafted, was rushed through the California legislature, and was quickly signed into law. After that, CCPA had to be amended further in 2018 and again in 2019. Many other proposed revisions to CCPA weren’t made. Nevertheless, CCPA only became effective last month on January 1, 2020 even though the rules and regulations for CCPA haven’t been finalized. Because of ambiguities and clarifications that still need to be resolved regarding CCPA’s far-reaching and sweeping policy and compliance provisions, CCPA is considered by many to be unfinished and untested. The full impact and ramification of CCPA have yet to be seen.

While there are many amendments to this Bill which should be made, at this juncture, we offer only the following three proposals (and we reserve the option to add more revisions in the future):

1. Beginning on page 29, line 19 through page 30, line 2, subsection (c) should be amended to read as follows:

(c) This part shall not apply to ~~personal information collected, processed, sold, or disclosed pursuant~~ a financial institution or an affiliate of a financial institution that is subject to the federal Gramm-Leach-Bliley Act (P.L. 106-102), and implementing regulations, to the extent this part is in conflict with that law.

The federal Gramm-Leach-Bliley Act governs the treatment of nonpublic personal information about consumers by financial institutions. It requires financial institutions (companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance) to explain their information-sharing practices to their customers and to safeguard sensitive data. Regulation P, which

implements the Act, was recodified by the Consumer Financial Protection Bureau. Regulation P establishes rules governing the duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information.

Because financial institutions are already subject to the federal law and federal regulation governing the privacy of personal information, the above proposed amendment is needed to clarify the entity-level exemption for financial institutions and their affiliates from this Bill.

2. On page 12, line 1, the definition of “consumer” should be amended to read as follows:

“Consumer” means ~~an individual residing in the State~~ a natural person who is a resident of the State and acting only in an individual or household context; it does not include a natural person acting in a commercial or employment context.

The present definition of “consumer” in the Bill is too broad and would unnecessarily include an individual who isn’t acting in their personal capacity. As drafted, this Bill would include an individual acting in an employment or in a commercial context. The above proposed amendment to the definition of “consumer” that we’re offering is based on a Washington state legislation.

3. The effective date of this Bill in Section 12 on page 59, beginning on line 16, should be “defected”.

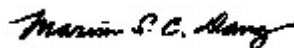
The Bill currently states that this Act would take effect “upon its approval”, provided that part III (which is for “data brokers”) would take effect on January 1, 2022.

As stated earlier, this Bill is modeled on the California Consumer Privacy Act which is still unfinished and untested. It was enacted in 2018 and became effective on January 1, 2020. Rules and regulations are being drafted.

An effective date for this Bill of “upon its approval” is not enough time to be in compliance.

We suggest putting in a “defective” effective date here to encourage further discussion.

Thank you for considering our testimony.



MARVIN S.C. DANG  
Attorney for Hawaii Financial Services Association





Tammy Cota, Executive Director  
1 Blanchard Court, Suite 101  
Montpelier, VT 05602  
802-279-3534  
[tammy@theinternetcoalition.com](mailto:tammy@theinternetcoalition.com)  
[www.theinternetcoalition.com](http://www.theinternetcoalition.com)

February 24, 2020

Honorable Chris Lee, Chair  
House Judiciary Committee, Room 433  
Honolulu, HI 96813

Honorable Roy Takumi, Chair  
House Consumer Protection and Commerce Committee, Room 320  
Honolulu, HI 96813

**RE: Opposition to HB 2572, Relating to Privacy**

Dear Chairman Lee and Chairman Takumi:

I am the executive director of the Internet Coalition (IC), a national trade association that represents members in state public policy discussions. The IC also serves as an informational resource, striving to protect and foster the Internet economy and the benefits it provides consumers.

The IC wants to express **opposition to HB 2572**, as this bill contains several provisions modeled after the California Consumer Privacy Act (CCPA), a problematic privacy law that is still in flux and largely untested as only parts of the law have been in effect since January 1 and further draft regulations are currently under consideration.

Protecting customer privacy and adhering to strong consumer privacy protections are an essential element in building and maintaining consumer trust. However, the IC urges you NOT to make the same mistakes as California lawmakers did in rushing to enact another seriously flawed and convoluted law which would impose overly burdensome and shockingly expensive compliance mandates on industry.

The CCPA is extremely costly for companies wanting to do business in California. According to the California Department of Justice's (DOJ) own estimates, it is expected to impact between 15,000 and 400,000 businesses, over half of which were identified as small companies. The initial business compliance costs are expected to total \$55 billion and rise by \$16.5 billion over the next 10 years. Despite some sections of this law becoming effective on January 1, the California Attorney General has yet to finalize proposed regulations. Left without clarity to many of the complex provisions of the law, thousands of businesses remain uncertain about their ultimate compliance obligations. Since companies and consumers still do not fully understand the entire implications of the CCPA, it is not ready for prime time and should not be used as a model for other states.

HB 2572, which mirrors many of the same problems as the CCPA, goes even further by specifically and separately addressing geolocation data and browser privacy. It is extremely confusing to propose comprehensive privacy legislation for all personal information, but it creates even more consumer confusion to separate out a few types of data that must held to

different standards. While we do not oppose opt-in consent to the sale of precise geolocation information, this bill would expand the consent to a broad range of daily transactions that would adversely impact the average consumer experience.

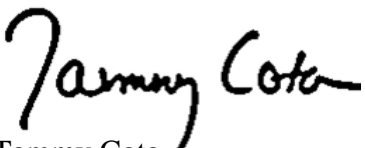
More importantly, the costly mandates of the CCPA, several of which are duplicated in HB 2572, would create significant regulatory obstacles to all companies doing business in Hawaii, but it will fall hardest on small to medium size businesses while deterring new, innovative start-up companies. In 2017, there were 126,600 small businesses in Hawaii which represents 99.3 percent of all businesses. These companies employ over 267,000 people, which is 51.6 percent of the local workforce. They also represent 86.5 percent of exports from Hawaii. The State of Hawaii should not be the first state to follow California's privacy law, which is not yet a finished product, presents significant unintended consequences and would impose unsustainable costs on Hawaii's businesses.

Further, the section of HB 2572 governing browser history conflicts with the FTC's Privacy Framework, which does not consider this type of data as sensitive or requiring a specific opt-in consent.

For all of these reasons, we urge you to **REJECT HB 2572** and avoid unnecessarily harming the economy and the business community. IC stands ready to help craft a forward-thinking privacy law that ensures consumer privacy rights while being flexible enough to encourage industry innovation and growth.

Please let me know if you would like more information or have questions.

Sincerely,



Tammy Cota



Sarah M. Ohs  
Director of Government Relations  
[sohs@cdiaonline.org](mailto:sohs@cdiaonline.org)  
(202) 408-7404

Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

**LATE**

[WWW.CDIAONLINE.ORG](http://WWW.CDIAONLINE.ORG)

February 24, 2020

The Honorable Chris Lee  
The Honorable Roy Takumi  
Committee on Judiciary & Committee on Consumer Protection & Commerce  
Conference Room 329  
State Capitol  
415 South Beretania Street  
Honolulu, Hawaii 96813

***RE: HB 2572, HD 1- Relating to Privacy & Data brokers- Hearing 2/25/2020 at 3pm***

Dear Chairman Lee and Chairman Takumi:

I write on behalf of the Consumer Data Industry Association (CDIA) to express our opposition to House Bill 2572, HD1, an act concerning consumer privacy. While this bill strives to create privacy legislation aimed at protecting consumers, as drafted it has the potential to create significant unintended consequences that could undermine privacy and data security.

The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

We believe the solution to privacy concerns are best handled at the federal level rather than a patchwork of privacy regulations by the states. The federal government has regulated data privacy for decades and has taken a thoughtful approach in recognizing the different types of data collected and the different uses of that data at the sectoral level. This is important because not all sectors collect the same type of data or use it in the same manner. Therefore, it is difficult to apply a single regulatory standard that governs the uses of all data without potentially creating harmful, unintended consequences.

***Fair Credit Reporting Act***

All of our members are regulated under the Fair Credit Reporting Act (FCRA). The FCRA outlines the purposes for which a consumer report may be furnished to a requestor. Under the FCRA, consumers have the right to access all information in their credit reports, including the

sources of the information, and the right to disclosure of their credit scores. A consumer may request one free credit report, from each of the nationwide credit reporting agencies (CRAs), and free reports are provided monthly to millions of consumers through a variety of services. Consumers have the right to dispute the completeness or accuracy of information contained in their files. Once a consumer notifies the CRA of the dispute the CRA must reinvestigate and record the current status of the disputed information, or delete it from the record. The CRA must also notify the furnisher of the disputed data of the consumer's dispute.

Beyond providing information that allows individuals to access credit, insurance, screening for employment, the information contained in consumer credit reporting databases aid in many other ways. Location services is one of the ways our members' databases assist law enforcement and state agencies. For example, when police are trying to locate a fugitive or a witness to a crime, they will often rely on one of our members' databases to find a more accurate address to locate the individual.

Fraud Prevention is another way that CDIA members' data are beneficial to states. Prevention of unemployment fraud, workers' compensation fraud and tax fraud are a few areas where this data can be useful. For example, when an individual applies for unemployment benefits with a state, the state labor department can contract with one of our member companies and have the ability to do a search to see if that individual has W2 information reported elsewhere and is working. This can prevent fraud against the state. The same is true if someone has applied for workers' compensation benefits from the state, the individual's name can be searched by one of our members' databases to see if they are working elsewhere. Tax fraud is another area, someone could have the ability to claim a tax exemption in one state but when compared with our members' records one could find if the individual was living elsewhere and claiming that as a primary residence.

### ***Importance of exemption language-unintended consequences***

It is imperative that exemptions be considered to protect legitimate uses of data if this bill is to move forward. An example of potential harm that could happen if one does not take into account the different sectors and the specific uses for that data, is applying things, such as "the right to deletion" or the "right to review the information" of fraud prevention databases. Companies that provide essential information to government and law enforcement to assist with fraud prevention, such as prevention of unemployment fraud, workers' compensation fraud and tax fraud would be subject to a consumer's ability to delete their information from those databases. The consequence of this would be that our member companies could no longer offer fraud prevention services to state agencies, without first tipping off the individual in question, who was potentially trying to defraud the state. In addition, if a consumer has objected to a service provider processing their personal data, it is much easier for that person to encounter identity fraud. This is because the

information used to verify the individual would no longer be available in our members' databases as a resource to confirm one's identity. Thus, making it easier for someone to steal another's identity.

However, even when a comprehensive privacy bill recognizes that exemption language is necessary, for things such as fraud, the FCRA, the Gramm-Leach-Bliley Act (GLBA), and public records, getting those exemptions properly written matters. For example, the current FCRA exemption in this bill is incomplete and could potentially cause problems for consumers. The FCRA exemption as currently drafted, is based on the original version of California's Consumer Privacy Act (CCPA) which was amended and corrected before the CCPA went into effect in January of this year.

Another example of an unintended consequence in this legislation, is that this bill does not have a complete GLBA exemption. Companies who share information with banks for anti-money laundering purposes without a "use-based" exemption would be unable to share that information where a consumer has objected to processing. This is because it is the bank's legal obligation that is covered by the exemption and not a third party. Under this scenario, banks themselves do not possess all of the data needed to comply with "know your customer" rules without third party data for comparison.

Further, the broad definition of "consumer" in the bill would subject commercial and employment data to deletion and access rights. Absent a distinction between an individual's professional and consumer life, all business-related information about an individual, and any associated information about the business (including financial information, business records, and other non-consumer information), potentially could be deleted or prevented from being shared. A consumer-focused privacy law should be limited to an individual or household capacity. In addition, it is important that federal privacy law exemptions are applied to the entirety of the bill. As currently drafted these exemptions do not apply throughout the legislation. If there is recognition that federal privacy laws should be exempt from these state requirements then the exemptions should apply throughout the bill.

### ***Unnecessary Data Broker Requirements***

In addition, this bill is problematic because it offers a narrow definition of data broker and mandates unnecessary requirements that are unwarranted and impractical. While we are concerned about protecting personal and sensitive information, HB 2572 would require a data broker to register with the state and meet additional disclosure obligations, including proprietary information, beyond what any other type of business must provide for the same type of information. There is nothing inherently unique to a data broker's operation that should require a state registration or enhanced disclosure obligation. Imposing a registration and disclosure on a specific type of business model that is already subject to consumer privacy rights in the underlying bill does not further the protection of consumers.

This legislation also requires additional burdens on data brokers that are CRAs. This legislation requires CRAs to annually send disclosures to consumers regarding: a consumer's right to a free credit report; how to access another person's credit report without their permission; an explanation of security freezes; and notice consumers' that they have the right to file a complaint with the Federal Trade Commission. There is nothing unique to a CRA that is a data broker, that requires a need for such disclosures. Federal law already mandates many of these disclosures to consumers and we believe that many of these requirements are preempted. (see attached document) Mandating additional annual disclosures on businesses only consumes time and money on businesses, and has the potential to confuse consumers all without offering any additional protections to the citizens of Hawaii.

Our members take very seriously the concerns of privacy and data security and use data fairly, responsibly and thoughtfully. There is a long history of privacy regulations federally at the sectoral level that considers the unique needs of data used in each industry. I would encourage you to distinguish between these unique uses of data, and whether or not new regulations are necessary. Existing federal statutes govern most uses of data and how it is gathered, collected and disseminated. A bill that attempts to create one regulation, that is applied across all sectors, fails to distinguish the unique uses of data, and the existing federal statutes that regulate differing industries. Moreover, the way this bill is drafted, it is only regulating those in the data broker community that are already heavily regulated at the federal level. If the concern is that there is a need for transparency to regulate the data broker industry, we believe you should consider regulating those data brokers that are not currently regulated at the federal level. This would hold the entire data broker community to the same standard, rather than narrowing the definition, as this bill does, and only focuses on a portion of the industry that is already heavily regulated federally.

For these reasons above, we oppose HB 2572. Thank you for your consideration of our comments. I would be happy to answer any further questions the Committee might have.

Sincerely,



Sarah M. Ohs

*Director of Government Relations*

### Proposed Section 25(a) Consumer Disclosures

The FCRA preempts proposed section 25(a) because it proposes to (1) require nationwide and nationwide specialty consumer reporting agencies to provide for the disclosure of information the agency has collected on the consumer, (2) require the disclosure of credit scores collected by consumer reporting agencies, and (3) impose requirements with respect to credit score disclosures that conflict with the FCRA.

**File disclosures by nationwide and nationwide specialty consumer reporting agencies.** First, the FCRA preempts state laws that impose any requirement with respect to nationwide and nationwide specialty consumer reporting agencies providing file disclosures once per year without charge. FCRA section 625(b)(5)(E) provides that state laws are preempted with respect to the conduct required by FCRA section 612(a), which requires that nationwide and nationwide specialty consumer reporting agencies provide file disclosures once per year to consumers without charge. 15 U.S.C. § 1681t(b)(5)(E). HB 2572 proposes to require any data broker, including nationwide and nationwide specialty consumer reporting agencies, to disclose “all information that the data broker has collected” about the consumer at the time of the request. Proposed section 25(a). HB 2572 proposes to regulate the conduct required by FCRA section 612(a) because it requires nationwide and nationwide specialty consumer reporting agencies to provide for the disclosure of information that overlaps and conflicts with section 612(a) and with timing requirements that differ from FCA section 612(a).

**Credit score disclosures.** Similarly, the FCRA preempts state laws that impose requirements with respect to credit score disclosures. FCRA section 625(b)(3) provides that state laws are preempted with respect to disclosures of credit scores by consumer reporting agencies under FCRA section 609(f) and (g). 15 U.S.C. § 1681t(b)(3). HB 2572 proposes to require that any data broker, including consumer reporting agencies, provide to consumer all information that the data broker has collected at the time of the request. Proposed section 25(a). HB 2572 proposes to impose requirements with respect to credit score disclosures because it proposes to require that a consumer reporting agency disclose all credit scores collected by consumer reporting agencies.

**File disclosure requirements that conflict with the FCRA.** Finally, the FCRA preempts state laws that conflict with the FCRA. FCRA section 625(a) preempts any state laws to the extent that those laws are inconsistent with the FCRA. 15 U.S.C. § 1681t(a). Among other things, the FCRA requires consumer reporting agencies to, upon a proper request, provide a disclosure of the consumer’s file with the consumer reporting agency, permitting the consumer reporting agency to withhold certain items of information. HB 2572 proposes to require that data brokers, including consumer reporting agencies, disclosure to consumers upon request all information that the data broker has collected at the time of the request. Proposed section 25(a). Because this proposed section does not permit consumer reporting agencies to withhold certain items of information from file disclosures, as the FCRA permits, this section conflicts with the FCRA and is therefore preempted by it.

### Proposed Section 25(b) Notice of Consumer Rights

In addition to proposed section 25(a), the FCRA preempts proposed section 25(b) of HB 2572 because it proposes to (1) require consumer reporting agencies to provide consumers with notices of legal rights related to the FCRA, (2) regulate the subject matter of prescreening, and (3) require consumer reporting agencies to provide notice of consumers’ right to a security freeze.

**FCRA notice of consumer and identity theft victim rights.** First, the FCRA preempts state laws with respect to notices of consumer rights and identity theft victim rights under the FCRA. FCRA section 625(b)(3) preempts state laws with respect to disclosures of consumer and identity theft victim rights required by FCRA section 609(c) and (d). HB 2572 proposes to require consumer reporting agencies to provide notice to consumers of certain legal rights, including the “right to receive a free copy of their credit report” and that “a consumer may file a complaint” with the FTC relating to a violation of “a law regulated consumer credit reporting.” Proposed section 25(b). HB 2572 proposes to impose requirements with respect to consumer and identity theft victim rights provided by FCRA section 609(c) and (d) because it proposes to require consumer reporting agencies to provide in different format notice of various legal rights relating to the FCRA.

**Prescreening of consumer reports.** Second, the FCRA preempts any state law imposing any requirement with respect to the subject matter of prescreening. FCRA section 625(b)(1)(A) preempts state laws with respect to any subject matter regulated under FCRA section 604(c) and (e). FCRA section 604(c) and (e) regulate the subject matter of the prescreening of consumers by obtaining consumer reports as permitted by the FCRA. HB 2572 proposes to require consumer reporting agencies to provide notice of the circumstances under which a person may access another person’s credit reporting without their permission, which includes prescreening uses. Thus, HB 2572 proposes to regulate the subject matter of prescreening and, as a result, the FCRA preempts proposed section 25(b).

**FCRA notice of security freeze rights.** Finally, the FCRA preempts any requirement to provide notice of a consumer’s right to a security freeze. FCRA section 625(b)(5)(B) provides that state laws are preempted with respect to the conduct required by FCRA section 605A, which requires consumer reporting agencies to provide consumers with notice of their right to obtain a security freeze any time the consumer reporting agency is required to provide the consumer with a file disclosure. 15 U.S.C. § 1681t(b)(5)(B). HB 2572 proposes to require that consumer reporting agencies provide consumers with an explanation of a security freeze and consumers’ rights to such a security freeze. Thus, HB 2572 proposes to regulate the conduct required by FCRA section 605A because it proposes to require consumer reporting agencies to provide notice of consumers’ right to a security freeze. As a result, the FCRA preempts proposed section 25(b).



**HB-2572-HD-1**

Submitted on: 2/24/2020 4:08:23 PM

Testimony for JUD on 2/25/2020 3:00:00 PM

**LATE**

Submitted By	Organization	Testifier Position	Present at Hearing
Jalem Correia	SAG-AFTRA	Support	No

Comments:



1654 South King Street  
Honolulu, Hawaii 96826-2097  
Telephone: (808) 941.0556  
Fax: (808) 945.0019  
Web site: [www.hcul.org](http://www.hcul.org)  
Email: [info@hcul.org](mailto:info@hcul.org)



Testimony to the House Committees on Judiciary; and  
Consumer Protection and Commerce  
Tuesday, February 25, 2020  
State Capitol, Room 325

**LATE**

Testimony on Opposition to HB 2572, Relating to Privacy

To: The Honorable Chris Lee and Roy Takumi, Chairs  
The Honorable Joy SanBuenaventura and Linda Ichiyama, Vice-Chairs  
Members of the Committees

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League, the local trade association for 51 Hawaii credit unions, representing over 800,000 credit union members across the state.

We offer the following comments in opposition to HB 2572, Relating to Privacy. This bill (1) redefines "personal information" for the purposes of security breach of personal information law; (2) establishes new provisions on consumer rights to personal information and data brokers; (3) prohibits the sale of geolocation information and internet browser information without consent; (4) amends provisions relating to electronic eavesdropping law; and (5) prohibits certain manipulated images of individuals.

While we understand and appreciate the intent of this bill, we have concerns about the unintended consequences of this legislation. This bill seems to be largely modeled after the California Consumer Privacy Act (CCPA), which has had many problems in both implementation and interpretation. While we understand the desire to protect the privacy and information of consumers, we have concerns about the level of service credit unions will be able to continue to provide under this new law.

We agree with the amendments proposed by the Hawaii Financial Services Association.

Thank you for the opportunity to provide comments on this issue.

# IRON WORKERS STABILIZATION FUND

---

February 25, 2020

3:00 pm

**LATE**

House Committee on Judiciary  
House Committee on Consumer Protection and Commerce  
Conference Room 016  
State Capitol  
415 South Beretania Street

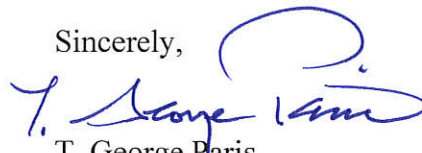
Re: HB2572, HD1 - RELATING TO PRIVACY.

Aloha Chair Chris Lee, Chair Roy Takumi, Vice-Chair Joy A. San Buenaventura, and Vice-Chair Linda Ichiyama and members of the House Committees on Judiciary and Consumer Protection and Commerce:

We **SUPPORT** the intent of HB2572 HD1. The bill, in enacted, redefines “personal information” for the purposes of security breach of personal information law. It further establishes new provisions on consumer rights to personal information and data brokers and prohibits the sale of geolocation information and internet browser information without consent, and amends provisions relating to electronic eavesdropping law. It finally prohibits certain manipulated images of individuals.

The House through HCR 225, SD 1 (2019) established the twenty-first century privacy law task force. The findings of this task force provides recommendations for the protection of the privacy of citizens in this digital age. We support the efforts of the task force, and especially the recommendation to protect individuals from the use of their images engaged in sexual conduct against their wishes. Such use of individuals images could threaten their careers and ability to earn a living in the future. Protect the privacy of our workers in this new digital age.

Sincerely,



T. George Paris  
Managing Director

TGP: MP



**LATE**

**TESTIMONY OF TINA YAMAKI  
PRESIDENT  
RETAIL MERCHANTS OF HAWAII  
February 25, 2020**

**Re: HB 2572 HD 1 RELATING TO PRIVACY**

Good afternoon Chairperson Lee and Chairperson Takumi and members of the House Committee on Judiciary and the Committee on Consumer Protection and Commerce. I am Tina Yamaki, President of the Retail Merchants of Hawaii and I appreciate this opportunity to testify.

The Retail Merchants of Hawaii (RMH) is a statewide not-for-profit trade organization committed to supporting the retail industry and business in general in Hawaii. The retail industry is one of the largest employers in the state, employing 25% of the labor force.

The Retail Merchants of Hawaii is opposed to HB 2572 HD1 Relating to Privacy. This measure redefines "personal information" for the purposes of security breach of personal information law; establishes new provisions on consumer rights to personal information and data brokers; prohibits the sale of geolocation information and internet browser information without consent; amends provisions relating to electronic eavesdropping law; and prohibits certain manipulated images of individuals.

Retailers main focus is to sell goods and services to our customers. Customers' expectations of retailers have changed by wanting seamless experience between online and instore shopping and retailers are trying to provide the customer service. Digital mobile technology has enabled retailers to innovate at a greater speed to meet the demands of consumers.

We feel that this type of legislation is premature as there are a lot of concerns being raised and should be addressed.

Retailers believe that all businesses handling personal information ought to have direct, statutory obligations to protect that information and honor consumers' rights with respect to it, including processing consumer rights requests. We do not support exemptions for businesses that have no other equivalent federal or state privacy obligations to protect data, such as the obligations provided by HIPAA and state laws covering protected health information. The burden should not fall solely on the consumer-facing companies like retailers to police downstream data use. The mere use of contractual language between retailers and their business partners does not sufficiently hold third parties and service providers accountable for assisting consumer-facing entities, particularly when honoring verified consumer rights requests, or in situations where the retailer is not party to a contract with a downstream vendor. Retailers will often be the first point of contact for customers about their personal information, but third parties and service providers handling their personal information should have equivalent statutory responsibility for their actions and fulfilling consumer rights requests.

Retailers should not be prohibited from offering different prices, rates, levels or qualities, of goods or services in the context of a customer loyalty program. Loyalty programs are not "financial incentives" and cannot be arbitrarily valuated by state-required mechanisms. Consumers voluntarily participate in loyalty programs and provide personal information so that they may earn benefits and discounts. A recent Forrester research study shows that 72% of adults participate in loyalty programs, and the average adult has signed up for programs with nine different businesses<sup>1</sup>. State laws should not make illegal the types of voluntary programs that

consumers love. Loyalty programs are a major component to many retailers' businesses. Opting into a rewards program at your favorite retailer can provide numerous benefits, including access to private sales, loyalty-based rewards and product discounts, invitations to special events with designers, and much more. Loyalty program participation is a relationship in which consumers receive tangible benefits in exchange for their personal information. These programs are typically offered free of charge and help bolster a relationship between customer and brand. It also ensures that brands can personalize and offer the best products that a consumer wants and needs - and when a customer no longer desires personalized advertisements, they should be empowered to opt out. Customer loyalty program membership increased by 15% between 2015 and 2017. Additionally, 87% percent of customer loyalty program members say they are open to sharing personal information about their activity and behavior in order to receive more personalized rewards. The widespread availability of personal information has increased concerns that this data will be used to discriminate against individuals, but retailers do not charge an individual a higher price for any product or service based on personal information relating to an individual's race, color, religion, national origin, sexual orientation, or gender identity.

Retailers support privacy legislation that recognizes that the channel or medium through which customers and businesses interact with each other, including physical locations, must be considered in designing compliant consumer privacy notifications and methods for businesses' secure receipt of consumer rights requests. This would ensure that both the privacy and security of those communications, and the timely processing of customer rights requests, are achieved in the manner most appropriate for each context. Taking requests in-store will mean creating additional verification processes which could pose additional security risks. Requiring in-store requests also imposes disproportionate obligations on brick-and-mortar stores, whose data processing is typically of low risk compared to big tech companies and systems (other than those designed to process payment card information) and may not be designed to facilitate processing personal information. Collection of information often takes place closer in time to the benefit provided to the consumer in offline interactions, making the use and purpose obvious.

Retailers in the last couple of years has seen a rise in organized retail theft. Those participating in organized retail crime range in age from elementary school students to the kapuna. Local companies have lost millions of dollars in the past year alone from shoplifters. With unemployment low, it is difficult to find qualified loss prevention personnel. Retailers rely on surveillance cameras to catch thieves.

This measure would be a big win and help the criminals who admit that shoplifting is their job and that they go to "work" daily - stealing products and items from our stores. With changing technology, surveillance cameras are stating to be able to recognize habitual criminals who enter the store and would be able to alert loss prevention personnel.

Asking a habitual shoplifter their permission to use facial recognition software is not an option. Passing this measure would be in the favor of and just be another win for criminals and a loss for businesses and the community.

We ask you to hold this measure

Mahalo for this opportunity to testify.

**HB-2572-HD-1**

Submitted on: 2/24/2020 2:39:14 PM

Testimony for JUD on 2/25/2020 3:00:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Serena Flores	Individual	Support	No

Comments:

February 24, 2020

H.B. 2572 Relating to Privacy

Committee: House Committees on Judiciary and Consumer Protection & Commerce

Hearing Date/Time: Tuesday, February 25, 2020, 3:00 p.m.

Place: Conference Room 329, State Capitol, 415 South Beretania Street

Dear Chairs Lee and Takumi, Vice Chairs San Buenaventura and Ichiyama, and members of the House Committees on Judiciary and on Consumer Protection & Commerce:

I write in **support** of H.B. 2572 Relating to Privacy.

As a privacy expert, I have worked in the field of data privacy for over 15 years and am a member of the 21st Century Privacy Law Task Force, created last year by HCR 225.

If you have one take away from today's discussion, I hope it is this: **Comprehensive state privacy laws are gaining momentum across the US, and we have to act for Hawaii residents to get these rights, too.**

In 2002, California passed the nation's first data breach notification law. Hawaii followed in 2006. By 2018, all fifty states had such laws. Without them, most companies had no obligation to tell consumers when their data was hacked, and we would never have learned of major data breaches like Target and Equifax, affecting 41 million and 147 million consumers respectively.

In 2018, California passed the California Consumer Privacy Act (CCPA). This was the first comprehensive privacy bill in the US. It established a consumers' right to control their own data. In 2019, eighteen states including Hawaii proposed similar legislation, and two states enacted smaller laws. In 2020, the count is now up to twenty-three states.

The California privacy law went into effect last month. Just like when the breach notification law passed in 2002, most companies are only offering these privacy rights to California residents. For instance, the Equifax privacy statement says:

## California Residents

The below section supplements our privacy statement to provide California residents with the information needed to exercise their rights under the CCPA.

The people of Hawaii deserve the same rights as the people of California. It will take Hawaii law to extend these rights to us. It's time to update our privacy laws to get these rights.

Thank you for your consideration and the opportunity support this legislation.



Kelly McCanlies

Fellow of Information Privacy, CIPP/US, CIPM, CIPT



**HB-2572-HD-1**

Submitted on: 2/24/2020 1:46:14 PM

Testimony for JUD on 2/25/2020 3:00:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
jess lundgren	Individual	Support	No

Comments:

This is a terrible misuse of technology , a slanderous & basically identity theft at a very high level. Victims should be greatly compensated & have reputations cleared



**LATE**

**HB-2572-HD-1**

Submitted on: 2/24/2020 3:03:05 PM

Testimony for JUD on 2/25/2020 3:00:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Leanne N. Teves	Individual	Support	No

Comments:

**LATE**

**HB-2572-HD-1**

Submitted on: 2/24/2020 3:36:02 PM

Testimony for JUD on 2/25/2020 3:00:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Jason Cutinella	Individual	Support	No

Comments:

Aloha,

Thank you for addressing this important issue about privacy.

**LATE**

I am in support of SECTION VI of this bill, found on page 58. I am in support of making the creation and distribution of deepfake pornography a felony.

As a SAG-AFTRA actress, I've seen how this has affected my fellow actors and could potentially impact me personally. Please note that deepfake pornography has been made of over 1,000 SAG-AFTRA members and is being used to harass college students and ex-girlfriends.

This privacy protection is a basic human right to be free from abuse and harassment

Mahalo for your time and consideration.

Jean Simon  
4944 Kilauea Ave Apt 2  
Honolulu, HI 96816

Rep. Chris Lee, Chair  
Rep. Joy A. San Buenaventura, Vice Chair  
House Committee on Judiciary



Jael Makagon  
Senior Privacy Analyst, Santa Clara County

February 25, 2019

Support with suggested amendment on H.B. No. 2572, H.D. 1, Relating to Privacy

Aloha Chair Lee, Vice Chair San Buenaventura, and Members of the Committee,

I am pleased to write in support of H.B. No. 2572, H.D. 1. I submit this testimony on behalf of myself individually and provide my institutional affiliation for identification purposes only.

As this Committee considers the passage of H.B. No. 2572, H.D.1, governmental bodies across the United States, from states to the smallest municipalities, are passing privacy legislation at a rapid rate. There is good reason for this activity. The promise of internet-based technologies has led to a steady erosion of privacy, which in turn has profound impacts on individuals and our democratic system.

Whether it is Target's marketing department identifying women in their second trimester as being particularly susceptible to ads,<sup>1</sup> or Cambridge Analytica using social media profiles in an attempt to influence and manipulate voters, the axiom holds true: information is power. The more information collected about people, including their online browsing activity, their location data, and the myriad other kinds of information that are now available through the use of networked devices, the greater the power that the holders of that information have over individuals.

People should not be forced to choose between access to digital services on the one hand and unfettered use of their personal information on the other. In reality this is no choice at all, because it is difficult if not impossible to participate in modern society without using or being tracked by networked devices in some way. But absent meaningful regulation that protects the right of the people to privacy as guaranteed in Article I, Section 6 of the Hawai'i Constitution, the status quo is unlikely to change.

H.B. No. 2572, H.D. 1 takes meaningful steps toward confronting this Hobson's choice. Among other things, it recognizes that geolocation information and internet browser information are particularly sensitive types of personal information that should not be sold without consent. It also requires data brokers, who collect and sell vast amounts of personal information but who

---

<sup>1</sup> Charles Duhigg, How Companies Learn Your Secrets, New York Times, Feb. 16, 2012.

typically have no direct relationship with consumers, to identify themselves and provide information on opting out of data collection. These regulations are a promising move toward addressing the startling asymmetry of power that exists in today's internet-based economy.

#### Suggested Amendment

Currently, H.B. No. 2572, H.D. 1 provides the Attorney General with sole enforcement power for violations of its provisions. This is a large burden for the Attorney General to bear, which is why in California, during the passage of its new privacy law (the California Consumer Protection Act), the state's Attorney General pushed for the addition of a private right of action. The effort ultimately failed, but the point remains: for the law to be effective, it needs to be enforced. The same holds true for this bill. The Committee should consider amending H.B. No. 2572, H.D. 1 to expand enforcement authority to Prosecuting Attorneys and Corporation Counsel.

I thank the Twenty-first Century Privacy Law Task Force for its work on this important issue, and I urge the committee to pass H.B. No. 2572, H.D. 1. Thank you for this opportunity to testify.

Jael Makagon

A handwritten signature in black ink, appearing to read 'J. Makagon', with a stylized, flowing script.

**LATE**

**HB-2572-HD-1**

Submitted on: 2/25/2020 10:52:23 AM

Testimony for JUD on 2/25/2020 3:00:00 PM

Submitted By	Organization	Testifier Position	Present at Hearing
Jay Fidell	Individual	Oppose	No

Comments:

TO THE CHAIR AND MEMBERS OF THE COMMITTEE:

I have been a member of the Privacy Task Force. In response to its recent Report and in connection with this bill, here are the points I last urged for further discussion by the Task Force and the Legislature:

1. The definition of the term "information." I am hoping we can discuss any unintended consequences of the proposed change in the definition of information.
2. The broker registration bill. I am concerned that the proposed data broker registration statute will be a burden and unfunded expense for the state agencies that might be called to enforce it. I think we can make a more compact and efficient statute which will be more practical for our state and the capacity of our state government.
3. The warrant notification arrangement. I am hoping we can discuss whether the government might somehow be able to extend the delayed warrant notification arrangement to civil scenarios, and how that can be avoided.
4. I also feel the task force should study national privacy, bullying, abuse and disinformation issues that have been raised nationally but which Congress has not addressed. Hawaii can contribute to the national conversation and could even be a leader in the field.

I would therefore want to see the task force, or a further iteration of the task force, meet again to cover these things before any action by the Legislature.

Thanks for your consideration on my views.

Jay Fidell



**LATE**

Committee: Committee on Judiciary  
Committee on Consumer Protection & Commerce  
Hearing Date/Time: Tuesday, February 25, 2020, 3:00 p.m.  
Place: Conference Room 329  
Re: Testimony of the ACLU of Hawai'i with comments on H.B. 2572, H.D. 1, Relating to Privacy

Dear Chair Lee, Chair Takumi, and committee members:

The American Civil Liberties Union of Hawai'i ("ACLU of Hawai'i") writes **with comments regarding H.B. 2572, H.D. 1**. While the ACLU of Hawai'i generally supports the intent of the bill, pending a more thorough analysis of the different provisions, we write specifically in support of Part IV of H.B. 2572, H.D. 1, which prohibits the sale or offering for sale of geolocation data and internet browser information without the explicit consent of the device user or subscriber. To further strengthen this section, we respectfully suggest that the committees consider adding language specifying that consent to the sale of geolocation or internet browser data cannot be a condition of use or subscription.

Hawai'i has a strong history of protecting an individual's right to privacy. Indeed, article 1, section 6 of our state constitution provides that "[t]he right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest." But the tracking of people's location constitutes a significant invasion of privacy. Tracking data can reveal many things about our lives, such as what friends, doctors, protests, meetings, political activities, support groups, or religious institutions we visit. The same is true for our internet browser history. And it is this personal information that companies share about us when they sell our data. Part IV of H.B. 2572, H.D. 1 protects these privacy interests by prohibiting the sale or offering for sale of this information without the *explicit* consent of the device user or internet subscriber.

To underscore the urgency of this issue, we refer you to a December 10, 2018 New York Times article entitled [Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret](#). As the article notes:

The millions of dots on the map trace highways, side streets, and bike trails — each one following the path of an anonymous cellphone user.

One path tracks someone from a home outside Newark to a nearby Planned Parenthood, remaining there for more than an hour. Another represents a person who

American Civil Liberties Union of Hawai'i  
P.O. Box 3410  
Honolulu, Hawai'i 96801  
T: 808.522-5900  
F: 808.522-5909  
E: [office@acluhawaii.org](mailto:office@acluhawaii.org)  
[www.acluhawaii.org](http://www.acluhawaii.org)

travels with the major of New York during the day and returns to Long Island at night.

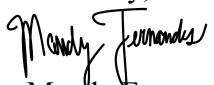
Yet another leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her.

**An app on the device gathered her location information, which was then sold without her knowledge.** It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The New York Times. While Ms. Magrin's identity was not disclosed in those records, The Times was able to easily connect her to that dot.

The Times reported that in about four months' of data they reviewed, Ms. Magrin's location was recorded over 8,600 times – on average, once every 21 minutes.

This type of intrusion is why we especially support the provision of H.B. 2572, H.D. 1 that notes information cannot be sold without the *explicit* consent of the individual. This provision clarifies that broad contracts of adhesion that are often part of cell phone contracts – often referred to as “user agreements” – which are rarely read by consumers, are insufficient to secure the consent required to share their location data pursuant to this bill. To further achieve the intent of this section, the committees may want to consider adding language clarifying that consent is void if granting consent to the sale of geolocation data or internet browser data is a condition of use of the service or product.

Thank you for the opportunity to testify.

Sincerely,  
  
Mandy Fernandes  
Policy Director  
ACLU of Hawai'i

*The mission of the ACLU of Hawai'i is to protect the fundamental freedoms enshrined in the U.S. and State Constitutions. The ACLU of Hawai'i fulfills this through legislative, litigation, and public education programs statewide. The ACLU of Hawai'i is a non-partisan and private non-profit organization that provides its services at no cost to the public and does not accept government funds. The ACLU of Hawai'i has been serving Hawai'i for over 50 years.*

American Civil Liberties Union of Hawai'i  
P.O. Box 3410  
Honolulu, Hawai'i 96801  
T: 808.522-5900  
F: 808.522-5909  
E: [office@acluhawaii.org](mailto:office@acluhawaii.org)  
[www.acluhawaii.org](http://www.acluhawaii.org)